WAVELET DOMAIN SCRAMBLING FOR IMAGE-BASED AUTHENTICATION

Giaime Ginesu[†], Student Member, IEEE, Daniele D. Giusto[†], Senior Member, IEEE and Tatiana Onali[†]

ABSTRACT

A simple image scrambling method for image-based authentication (IBA) is proposed and evaluated. The devised scheme may be embedded into any wavelet-based IBA framework to provide mutual authentication with challenge-response architecture. The severe constraints on security, data transmission capability and user friendliness are addressed by the complete system, especially in the wireless environment. Data and application scalability is provided through the JPEG2000 standard and JPIP framework.

1. INTRODUCTION

The most part of current authentication systems, as alphanumeric passwords, are capable of guaranteeing the identity of user only (weak authentication). New client-server applications require a further security level. Verified authenticity of service providers becomes essential to avoid the risk of coming up against a shadow server. More advanced solutions have been proposed in order to achieve authentication of both user and server (mutual or strong authentication). In general, such methods provide data encryption through secret keys and challenge-response mechanism. These systems offer a good level of security, but may require additional hardware support, as encryption-calculators, tokens or smart cards, which are often expensive and incompatible with new network technologies. An alternative solution for generating challenge-response schemes is to use steganography, watermarking or image scrambling techniques. They allow inserting some secret visual information into the message using a key for mutual authentication.

Some visual login systems based on encryption algorithms have been proposed in the literature. An example of visual cryptography [1, 2] provides each user with a transparency, i.e. a portion of visual information, which reveals a secret when combined with another sent by the server during authentication. Steganography may be used together with visual cryptography [3]. The most widely known technique consists in replacing the last bit of each image pixel with a bit of secret information. These systems rely only on the secret keys exchange; one key is stored into the user terminal, while the other is sent by the server at each login request. Both user and server keys are then unprotected against theft or network sniffing attacks, allowing malicious clients or shadow servers to break the security system.

This paper proposes a simple image scrambling method to be adopted for mutual authentication in a image-based authentication framework: server and user share a secret key which is transmitted once during the registration phase and allows the encryption and decryption of any visual information transmitted by server to client. Such challenge-response scheme is coupled with the image-based authentication (IBA) technique described in [4]. Besides mutual authentication, the proposed method results in the increase of user authentication security without compromising simplicity and efficiency of the devised scheme. The proposed framework makes extensive use of the JPEG2000 standard both for image storage and processing, while relying on the properties of wavelet decomposition for the scrambling and transmission of visual information to the client.

The paper is organized as follows; Section 2 briefly describes the adopted IBA framework. The proposed image scrambling method for mutual authentication is described in Section 3. Finally conclusions are drawn.

2. IBA FRAMEWORK

The proposed IBA method is based on a client-server interface and provides a two factor authentication, relying on a graphical password and a shared secret key. The core algorithm is described in [4]. It consists in a visual challenge-response architecture, which requires the user to recognize a combination of pass-images and pass-details through an iterative selection and zooming. This graphical password technique is supported by the JPEG2000 standard: the use of tiling and JPIP protocol allows for data-stream scalability and for the efficient transmission of image information. Through evaluation and comparison with the state of the art IBA techniques, the proposed visual login system has proven to offer good average performance. Moreover, it constitutes an excellent trade-off between security, data transfer and usability, also in wireless environment, which imposes severe constraints

[†] MCLab, Department of Electrical and Electronic Engineering, University of Cagliari, piazza d'Armi, 09123, Cagliari, Italy

on security, bandwidth capability and user friendliness. In order to provide mutual authentication, fundamental for new web applications, the IBA password technique has been complemented with a challenge-response scheme based on a secret shared secret key for image scrambling.

During the registration phase, the server defines a scrambling key, derived from a mixture of personal information and random data, such as the current time or the actual content of a few bytes of RAM. This key is shared by both server and client and is transmitted only during the registration phase. It is used for generating the pseudo-random sequence that drives the image scrambling process discussed in Section 2. During the authentication process, each time the user requests any visual information, the server provides its encrypted version with the scrambling key. Then, the client must descramble the visual information in order to make its content understandable and select its graphical password. In this way, not only mutual authentication is guaranteed, but also security of user authentication is improved. Fig. 1 compares the security of simple IBA method, in terms of possible password combinations, with security of mutual IBA based on a scrambling key, in the cases of 30 and 50 characters long key. An average wireless application profile is considered by adopting one pass-images sequence only for image selection and four 4x4 grids for each detail selection step.

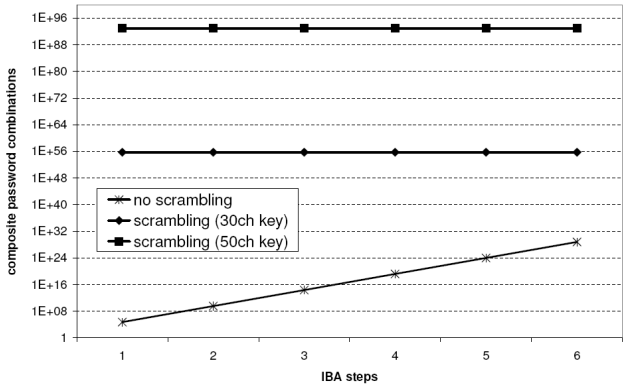

Fig. 1. Security of the proposed method without and with scrambling.

3. IMAGE SCRAMBLING TECHNIQUE

The devised system relies on image data scrambling for transmitting the visual information from server to client and supporting the mutual authentication feature.

Several image scrambling techniques have been investigated by the recent literature. They are generally based on the randomization of pixels ordering or on the addition of some variations in the coding algorithm. A process of lossless scrambling/descrambling is defined in [5], using a periodically shift variant (PSV) discrete system in order to change pixel disposition. In [6] a method based on chaos system is presented. [7] discusses two kinds of transformations, based on the Fibonacci and Lucas sequences. They totally decorrelate the visual signal, spreading all pixels, while maintaining equidistance as in the original image, and separating adjacent pixels as much as possible. In [8], the scrambling scheme relies on the 2D extension of the discrete prolate spheroidal sequences (DPSS) is proposed. Other methods define image scrambling in a transform domain. A JPEG-based image encryption algorithm has been proposed in [9]. It consists in three steps: the permutation of luminance and chrominance planes by pseudo-random SFCs (Space Filling Curves); the confusion of DCT coefficients in each DCT block, based on different frequency bands; the encryption of DCT coefficient signs. For JPEG2000 images, scrambling methods are proposed in [10, 11]. [10] presents a system based on JPSEC that encrypts the packet body using RC4 and AES algorithms. In [11], a method for partial-scalable scrambling of JPEG2000 coding units, *i.e.* layers, DWT-levels, sub-bands or code-blocks, is proposed. It relies on public-key encryption, which is robust to attacks but requires much more computational cost than secret-key encryption.

Although the previous methods provide several good solutions for the encryption problem, their computational complexity is often high, so that their application may become critical in the case of mobile environment. A choice has been made to develop a simple, yet effective, method, based on the properties of wavelet decomposition. Such choice allows for a nice integration with state of the art coders, such as JPEG2000, and adds only an irrelevant computational cost to the codec. Moreover, the integration of coding and scrambling makes the system more robust to security attacks. As a drawback, the scrambling process inevitably reduces the wavelet ability to decorrelate the signal's energy, resulting in weakened coding efficiency. However, such aspect may be restrained so to offer an adequate perceived quality for reasonable compression ratios. In fact, it must be observed that the application of visual authentication is not particularly demanding in terms of high-quality visual reproduction. Thus, the proposed system is based on three stages of pseudo-random permutations in the wavelet domain: LL coefficients, high subbands blocks and high subbands signs (Fig. 2).

The Mersenne Twister pseudorandom number generator [12] is adopted in order to generate each scrambling pattern. Since each stage is meant to drive a particular class of coefficient permutations in the wavelet domain, the pseudorandom generator must provide three different sequences from the scrambling key defined during the registration phase. This is obtained by normalizing the MT output to a desired range that covers

each permutation's space, depending on image size and decomposition levels. The scrambling key constitutes the seed for the pseudo-random generator.

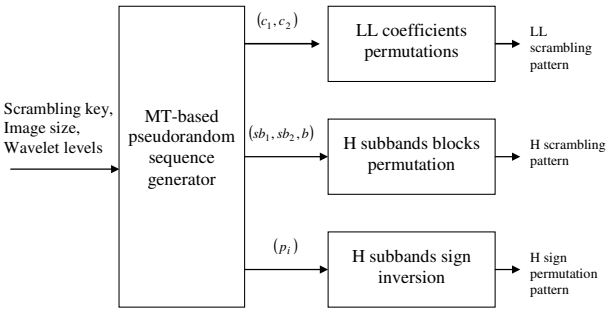

Fig. 2. Scheme for the scrambling method and resulting permutation patterns.

While LL coefficients permutation is straightforward, *i.e.* the sequence (c_1, c_2) defines which two coefficients to exchange inside the LL subband, high subband blocks permutation follows a different scheme. The sequence (sb_1, sb_2, b) defines which two subbands, sb_1, sb_2 and which reference block, b, from the largest subband among sb_1 and sb_2 to consider. Block size is proportional to the largest subband size, *e.g.* 2×2 blocks for 32×32 subbands, 4×4 blocks for 64×64 subbands, and so on, so that any subband is divided into 16×16 blocks in the case of square subbands.

Then, the algorithm searches for the block (target block) in the smaller subband, which satisfies the condition of having the least MSE in respect to the reference block. The two blocks of coefficients are then exchanged. Such simple procedure is summarized as follows:

For each (sb_1, sb_2, b):

$s_{\max} = MAX(sb_1, sb_2)$; $s_{\min} = MIN(sb_1, sb_2)$

$size_{\text{reference\_block}} = size_{\text{target\_block}} = size_{s_{\max}} / 16$

$position_{\text{reference\_block}} = b$

Find target_block in $s_{\min}$ that minimizes $MSE(\text{reference\_block}, \text{target\_block})$

Permute target_block and reference_block

Finally, sign inversion is driven by the index sequence p_i. The algorithm inverts the sign of the coefficient with greatest absolute value in a neighborhood of $(width_{subband}/16)\times(height_{subband}/16)$ coefficients centered on each index.

LL coefficients, H blocks and H coefficients involved into the permutation and sign inversion process are depicted in Fig. 3 as white pixels in the upper left corner, grey blocks and sparse clear pixels respectively.

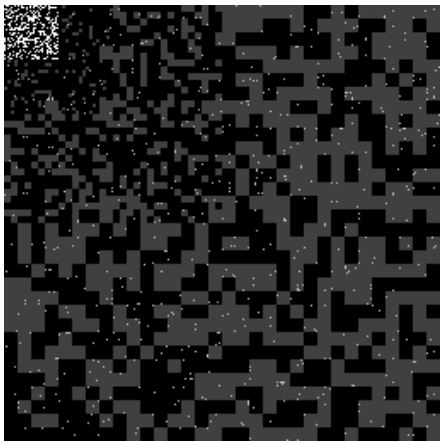

Fig. 3. Wavelet-domain permutation pattern.

Both H blocks permutation and sign inversion stages are implemented as a reasonable tradeoff between computational complexity, which is maintained very low, and minimization of the effect of scrambling on compression performance. In fact, the permutation of blocks with minimum MSE distance and sign inversion of locally maximum coefficients guarantees that the decomposed signal decorrelation is not dramatically reduced. Another interesting aspect of the proposed method is that the descrambling process simply follows the scrambling procedure by considering the permutation pattern in reverse order.

In order to evaluate the proposed algorithm in its application environment, 15 different test images have been considered. Each original image has been used to produce three reduced detail versions as defined by the IBA method considered. In Fig. 4 the average rate-distortion curve is shown, considering correct scrambling/descrambling and wrong or no descrambling. Although the scrambling/descrambling process has still an important effect on coding efficiency, *i.e.* there is an average deterioration of 5 to 8 dB compared to unscrambled coding, at a bitrate of 1.5bpp the system offers adequate image reproduction. This is also evidenced in Fig. 5, where a visual comparison between unscrambled, correctly descrambled and wrongly descrambled images is provided. It must also be observed that wrong or no descrambling, or equivalently wrong or no scrambling with correct descrambling, results in unintelligible image data, achieving a constant PSNR slightly inferior to 15dB.

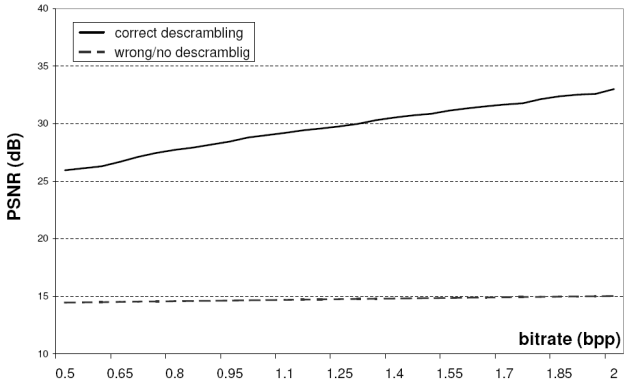

Fig. 4. Average coding results with correct or wrong/no descrambling.

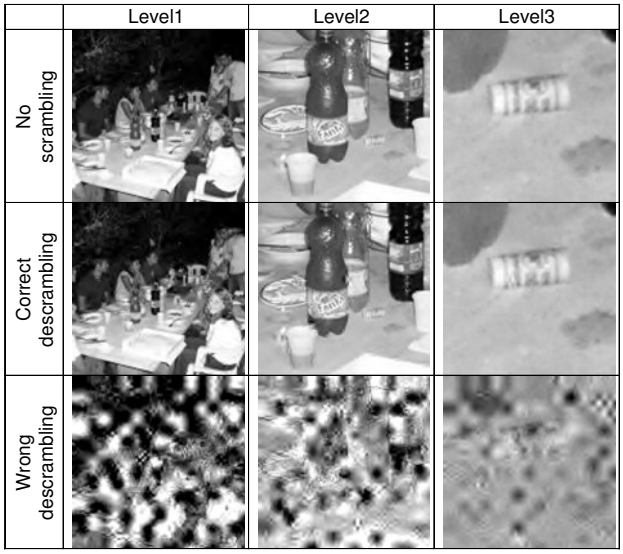

Fig. 5. Example of visual results for the scrambling technique, coded at 1.5bpp.

3. CONCLUSIONS

A simple method for wavelet-domain image scrambling has been presented. The proposed technique has been mainly conceived for embedding into image-based authentication application in order to provide mutual authentication feature. This solution allows to guarantee a high level of security, protecting the system against the risk of both malicious client and shadow server attacks. Moreover, the scrambling of transmitted visual information results in the reinforcement of the IBA system privacy and security. The proposed approach does not require either hardware upgrade or high computational capability and may be adopted by many application, also in wireless environment.

4. REFERENCES

[1] M. Naor and B. Pinkas, "Visual authentication and identification", in Burt Kaliski, editor, Advances in Cryptology, Crypto '97, pp. 322-336, Springer-Verlag, Berlin, 1997.

[2] M. Naor and A. Shamir, "Visual cryptography", in Alfredo De Santis, editor, Advances in Cryptology, EuroCrypt '94, pp. 1-12, Springer-Verlag, Berlin, 1995.

[3] M. Kharrazi, H.T. Sencar, and N. Memon, "Image Steganography: Concepts and Practice", Lecture Note Series, Institute for Mathematical Sciences, National University of Singapore, Apr. 2004.

[4] G. Ginesu, D.D. Giusto, T. Onali, "Application-Scalable Image-based Authentication Framework with JPEG2000," IEEE Int. Workshop on Multimedia Signal Processing, Shanghai, China, Oct. 30 – Nov. 2, 2005

[5] K.S. Joo and T. Bose, "Two-Dimensional Periodically Shift Variant Digital Filters", IEEE Trans. on Circuits and Systems for Video Technology, Vol. 6, No. 1, Feb. 1996.

[6] Z. Han, W.X. Feng, L.Z. Hui, L.D. Hai, L.Y. Chou, "A New Image Encryption Algorithm Based on Chaos System", Proc. IEEE Int. Conf. on Robotics, Intelligent Systems and Signal Processing, Changsha, pp 778-782, China, Oct. 2003.

[7] J. Zou1, R.K. Ward, D. Qi, "The Generalized Fibonacci Transformations and Application to Image Scrambling", Proc. Int. Conf. on Acoustics, Speech, and Signal Processing, pp 385-388, Montreal, May 2004.

[8] D. Van De Ville, W. Philips, R. Van de Walle, I. Lemahieu, "Image Scrambling Without Bandwidth Expansion", IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 6, pp 892-897, Jun. 2004.

[9] S. Lian, J. Sun, Z. Wang, "A Novel Image Encryption Scheme Based-on JPEG Encoding", Proc. the 8th Int. Conf. on Information Visualization, London, 2004.

[10] H. Wu and D. Ma, "Efficient and Secure Encryption Schemes for Jpeg2000", Proc. Int. Conf. on Acoustics, Speech, and Signal Processing, pp 869-872, Montreal, May 2004.

[11] O.Watanabe, A. Nakazaki, H. Kiya, "A Fast Image-Scramble Method using Public-Key Encryption allowing Backward Compatibility with JPEG2000", Proc. Int. Conf. on Image Processing, pp 3435-3438, Singapore, Oct. 2004.

[12] M. Matsumoto and T. Nishimura, "Mersenne Twister: A 623-dimensionally equidistributed uniform pseudorandom number generator", ACM Trans. on Modeling and Computer Simulation Vol. 8, No. 1, pp.3-30, Jan. 1998.