Multilayered Information Encryption Scheme with Fine-grained Authentication

Yi-Hui Chen*, Ching-Hu Lu† and Po-Yu Hsu*
* Asia University of M-Commerce and Multimedia Applications, Taichung, Taiwan
E-mail: chenyh@asia.edu.tw and jacky1772000@gmail.com, Tel: +886-4-23323456
† National Taiwan University of Science and Technology, Taipei, Taiwan
E-mail: jhluh@ieee.org, Tel: +886-2-27376988
† Correspondence author: Ching-Hu Lu (jhluh@ieee.org)

***Abstract*—Secret communication has long been an import issue in recent years. To protect a secret, encryption is a general way to help owners encrypt the secret into meaningless information for non-owners in order to prevent secret leakage. Since fine-grained encryption provides more flexibility in information protection, it has drawn more attention in recent years, but effective methods are rare in this new research domain. In this study, a multilayered and authentication-enhanced scheme for information encryption was proposed, and its application was focused on image encryption. The scheme encrypts the whole or parts of a secret image according to its owners' authorization. Owners of the image can also specify their own permissions encrypted in the image by embedding the corresponding authentication codes into the encrypted image. Later, the receivers can extract the hidden authentication codes to judge whether the decrypted image is fake or not. The experiments have demonstrated the effectiveness of the proposed encryption scheme, and the conceptual framework can also be applied to other applications requiring information encryption.**

Keywords Secret Sharing; Double layered Image Encryption; Tag Image; Access control

I. INTRODUCTION

The Internet has the potential to greatly boost the convenience in our daily lives, but also increased the risk on privacy violation or secret leakage. For example, the interconnect cameras in a smart home can improve context-awareness and remote monitoring but at the risk of privacy violation. In this regard, secret communication has become an important issue in recent years, particularly for the upcoming era of IoTs (the Internet of Things). Among all possible exchanging information, image related data is more privacy sensitive, and that is why steganography is widely used to hide a secret into cover multimedia, such as images, audios, videos, etc. To protect the secret, encryption is another general way to help the owners encrypt a secret into meaningless noises and only the person who owns the secret key can decrypt the secret.

Information encryption was widely used in ensuring the quality of services in wireless communication as well. The resolution of a video service can be determined by how much a user is willing to pay [6], [9], [14], [15]. Also, the access control of resolution on a video can be used to prevent from plagiarism. However, the prior encryption schemes cannot be easily applied on some embedded devices because they needs powerful computation ability. In this regard, fine-grained based encryption schemes [7], [16], [17], [4] for image encryption were proposed.

In a social network, the owner of an image may need to share different parts of then image with different receivers. This is, the owner need to have the ability to authorize different receivers to access different contents on the same image, thus leading to so-called fine-grained access control. Fine-grained access control schemes [2], [3], [5], [10], [12], [13] are widely in current business models, such as publishing [1], authoring [5], E-services [1], [12], etc. However, the prior image encryption schemes focused more on how to encrypt a whole image, but did not support partial authorization.

A fine-grained encryption scheme is required in some domains, such as e-Papers, e-Books, collaborative design, and so on. More specifically, the policy of authorizing an image for children and adults should be different. Those images related to violence or pornography should be encrypted for children. People have no rights to see the contents without legitimate copyrights. Thus, a fine-grained access control scheme is desirable for image encryption, and it allows owners to encrypt different parts of an image according different authorizations.

The fine-grained encryption scheme proposed by [4] was achieved by modeling the sensitive regions using a tree structure. Next, the tree structure was transformed into a serial bit of compression codes. The compression codes in turn were hidden into the digital images and then shuffled the sensitive regions into noise pads. They protects the sensitive regions; however, the image needs to keep a huge amount of compression codes for identifying whereabouts of the sensitive regions.

To authenticate whether the received encrypted image was a fake one, new image authentication schemes [16], [17] were proposed. Note that the challenge of such authentication schemes is that the encrypted contents are changed after embedding authentication codes; thus, they may fail in an attempt to decrypt the contents. Therefore, these schemes require a reversible embedding or hiding technique to guarantee that the encrypted contents can be completely decrypted. However, the hiding capacity of the reversible hiding schemes is still limited and often with the underflow or overflow problems in the current studies [8]. To resolve this problem, the authors proposed a multilayer and fine-grained image encryp-

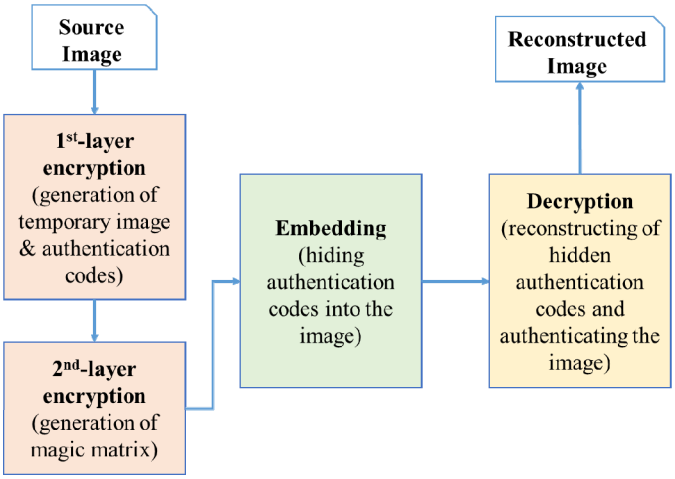


Fig. 1. The flowchart of the proposed approach.

tion scheme with the authentication ability to ensure the authenticity of a received image. The scheme adopts the method [11] from Lin et al. to design a reversible embedding approach for image encryption without suffering from the underflow or overflow problems. Also, the hiding capacity of Lin et al.'s scheme is greater than others. In addition, the fine-grained image encryption scheme is provided to allow the owners to encrypt any partial contents of an image in accordance with to their concerns in access control.

II. THE STEGANOGRAPHY SCHEME [11]

Lin et al. proposed a steganography scheme based on the concept of Sudoku. First, the secret bitstream s is transformed into a secret sequence of digits ss by using a 3^n-base notational system, and denoted as a pixel unit $x = (\beta_1, \beta_2, ..., \beta_n)_{3^n}$.

Next, each digit of x is hidden into the cover image by a pixel pair using an extracting function f, which is defined as:

$$f(\lambda_1, \lambda_2, ..., \lambda_n) = \sum_{i=1}^{n} 3^{i-1} \lambda_i \mod 3^n. \quad (1)$$

Here, n pixels be a group as input data depicted as $(\lambda_1, \lambda_2, ..., \lambda_n)$ in Equation (1). Suppose that a digit r, obtained by x, is to embed into the cover image. A temporary value y is generated with equation (2).

$$y = (r - f(\lambda_1, \lambda_2, ..., \lambda_n) + \left\lfloor \frac{3^n - 1}{2} \right\rfloor) \mod 3^n. \quad (2)$$

Next, the value of y is transformed into a sequence yy by using a 3^n-base notational system as $yy = s_1 s_2 ... s_n$, where $s_i \in [0, 1, \ldots, n-1]$ and $1 \le i \le n$. Subsequently, the sequence of each digit in yy is changed and subtracted by 1 to generate a new sequence as $z = e_n e_{n-1} ... e_1$, where $e_j \in [-1, 0, \ldots, n-2]$, $e_j = s_i - 1$, and $j = n - i + 1$. Finally, each digit in x is added to a corresponding digit in z with equation (3) to create a new pixel unit $w = (p_1, p_2, ..., p_n)$.

$$p_i = \lambda_i + e_i, \text{ where } i = 1 \text{ to } n. \quad (3)$$

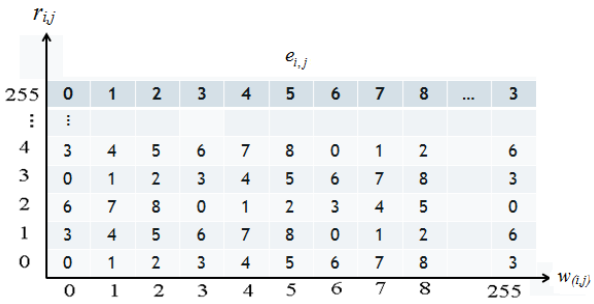


Fig. 2. Example of magic matrix.

When a receiver receives the $(p_1, p_2, ..., p_n)$, the decoder can extract the hidden secrets ss with equation (1), which replaces $(\lambda_1, \lambda_2, ..., \lambda_n)$ with $(p_1, p_2, ..., p_n)$. The secret s can be recovered by transforming ss with the 2-base notational system.

III. PROPOSED SCHEME

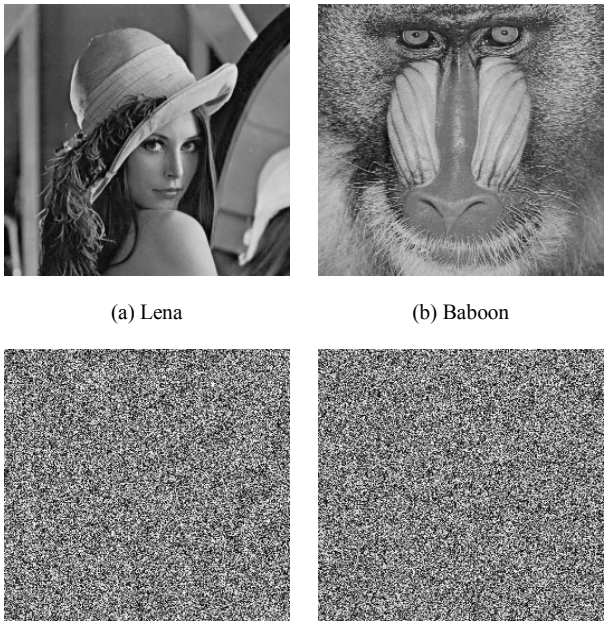
There are totally three procedures including encryption, embedding, and decryption, where a multilayered encryption method is proposed, and the first version has two layers, as illustrated in Fig. 1.

In the first layer of the encryption procedure, a secret image S is divided into several blocks with $w \times w$ pixels. Note that the q-th block is denoted as B_q, and (i, j) refers to the position of a pixel in B_q and its pixel value is denoted as $p_{i,j}$. A mask is used to indicate whether pixels $p_{i,j}$ in B_q is authorized. If authorized, $m_{i,j}$ equals to 1; otherwise, 0. The temporary image is generated with equation (4), where rnd_seed is a random integer ranging from 0 to 255, and $\oplus$ is the XOR (Exclusive-OR) operation. This is used to make the un-authorized regions as random pads, which are meaningless to users; otherwise, keep intact. After that, the pixels after first encryption phase, the pixel located at (i,j)-position is denoted as $t_{i,j}$.

$$t_{i,j} = \begin{cases} p_{i,j}, & \text{if } m_{i,j} = 1, \\ rnd\_seed \oplus p_{i,j}, & \text{otherwise.} \end{cases} \quad (4)$$

Next, the 2LSB (Least Significant Bit) of $t_{i,j}$ are replaced with 00, denoted as S'. The image S' is hashed to generate authentication codes A. Later, receivers can extract the hidden authentication codes to authenticate whether the image is not a fake.

Generally, the MSBs (Most Significant Bits) are the most important bits for a pixel. That is, if the MSB is changed, the original content cannot easily be recognized. On the contrast, the LSB is not important and if it is changed, the content still can be recognized. Thus, in the second layer of the encryption procedure, pixels $t_{i,j}$ are transformed into a binary stream and only the 3MSBs are used to encrypt. Note that the one who owns the secret key can decrypt the second layered encryption. For example, if the pixel value, denoted as $s_{i,j}$, is 201, the corresponding 3MSBs are 110. The 3MSBs are transformed into a decimal digit and denoted as $w_{i,j}$. In this example, $w_{i,j}$ is 6. The random number $r_{i,j}$ is generated and its interval is [0, 255]. A magic matrix is calculated with equation (1). In Fig. 2, we



(a) Lena (b) Baboon

(c) Shuffled image of Lena (d) Shuffled image of Baboon

Fig. 3. Shuffling the 3MSBs of the original images .

can use $r_{i,j}$ and $w_{i,j}$ to obtain $e_{i,j}$ with the magic matrix. If $e_{i,j}$ equals 8, it requires four MSBs; however, three MSBs are enough for this case. Thus, we can adjust $e_{i,j}$ value with equation (5). If $e_{i,j}$ equals 8, let $w_{i,j}$ be 8; then, we use $r_{i,j}$ and $w_{i,j}$ to obtain $e_{i,j}$ with the magic matrix again to complete the encryption procedure. For example, if $w_{i,j}$ and $r_{i,j}$ are 5 and 1, respectively, the mapping $e_{i,j}$ is equal to 8. Thus, let $w_{i,j}$ equal 8. The new $e_{i,j}$ (equals to 2) is obtained by mapping $w_{i,j}$ and $r_{i,j}$ (8 and 1, respectively) to magic matrix.

$$\begin{cases} \text{intact}, & \text{if } e_{i,j} \neq 8, \\ w_{i,j} = e_{i,j}, & \text{if } e_{i,j} = 8. \end{cases} \tag{5}$$

To avoid the authentication codes are easily extracted, encrypted results are used to shuffle the authentication codes as shown in equation (6), where every two bits of the authentication codes A are treated as a bit pair, denoted as $h_{i,j}$ and use equation (6) to calculate L_s value. Next, L_s is transformed into a two binary bits B_s. In the embedding procedure, the 2LSBs of the original pixel value are replaced with B_s.

$$L_s = (e_{i,j} + h_{i,j}) \bmod 4. \tag{6}$$

In the decryption procedure, the 2LSBs and 3MSBs are extracted and denoted as B_s' and $e_{i,j}'$, and the secret key is used to generate the $r_{i,j}'$. Later on, the mapping value, depicted as $w_{i,j}'$, can be extracted with the magic matrix according to $e_{i,j}'$ and $r_{i,j}'$ to reconstruct the secret image. Note that if $w_{i,j}'$ equals 8, we replace the value of $e_{i,j}$ with 8 to extract $w_{i,j}'$ again. For instance, if $e_{i,j}'$ and $r_{i,j}'$ are 2 and 1, respectively, $w_{i,j}'$ is then mapped as 8. Again, let $e_{i,j}'$ and $r_{i,j}'$ equal 8 and 1; $w_{i,j}'$ is identical to 5.

The hidden authentication codes $h_{i,j}$ are obtained by equation (6), where L_s and $e_{i,j}$ are the decimal value of B_s' and $e_{i,j}'$, respectively. The next step is concatenating all $h_{i,j}$ to reconstruct the authentication codes A'. The 2LSBs of the reconstructed image are substituted with 00 to create a new image W. The hash codes $\widetilde{A}$ are obtained by hashing W. Compare A' with $\widetilde{A}$ to check whether it is authentic. If A' equals to $\widetilde{A}$, it is judged as authentic; otherwise, inauthentic.

IV. Experimental Results

This section shows the experimental results and the performance of the proposed scheme. Two grayscale images with 256×256 pixels were used as the test images in the experiments, which were named "Lena" and "Baboon."

The figures illustrated in Fig. 3 are the results of the first experiment after shuffling the 3MSBs of the original images. The results show that the shuffled images are meaningless to users. Thus, we applied the results to evaluate the proposed double layered encryption scheme.

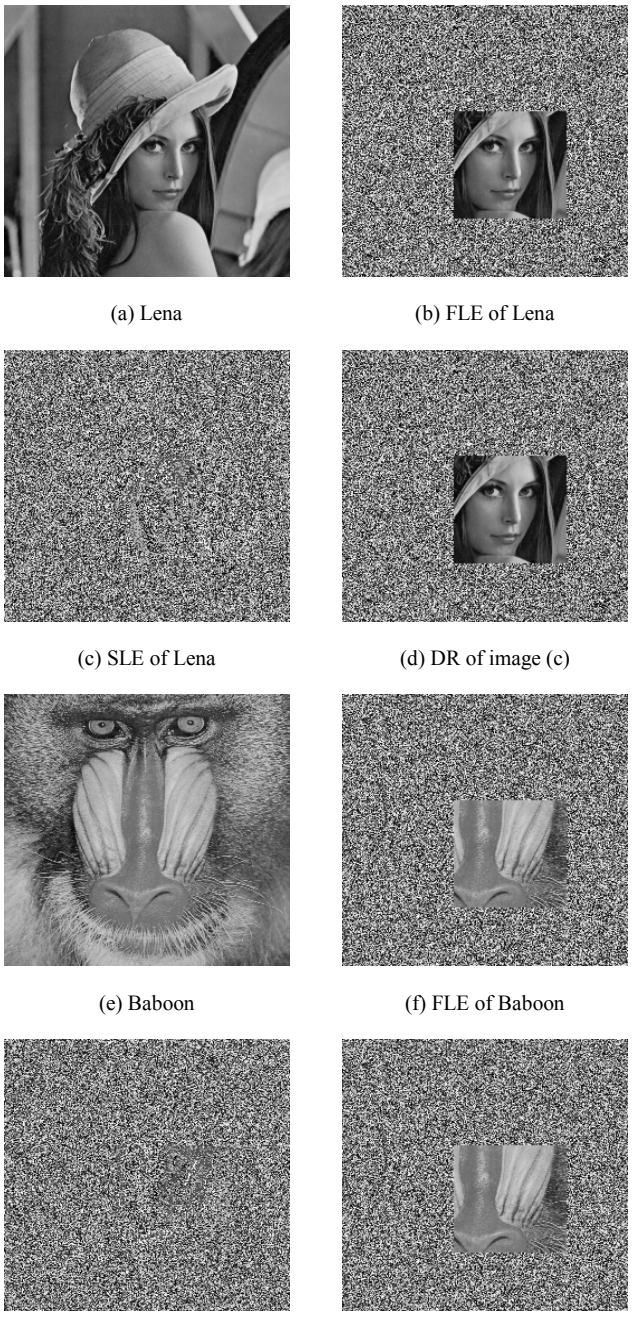
To measure the encryption and decryption abilities, two examples are shown in Fig. 4 (a) through (h). After the first layered encryption (abbreviated as FLE in the figures), the encrypted images are shown in Fig. 4 (b) through 3(f), where only the authorized regions are meaningful to users. After the second layered encryption (abbreviated as SLE in the figures), the encrypted results are shown in Fig. 4 (c) and Fig. 4 (g). After the decryption procedure, the decrypted results (DR for short) are illustrated in Fig. 4 (d) through (h). Only the authorized regions are readily recognizable with naked eyes, the others are meaningless.

As for the visual qualities (measured by PSNR), the image qualities of Fig. 4 (d) and Fig. 4 (h), compared to Fig. 4 (b) and Fig. 4 (f), are 69.40 dB and 69.91 dB, respectively. The results show that the decrypted images can provide good visual qualities for users to clearly identify the authorized regions of interest.

V. CONCLUSIONS

In this study, a new scheme in image encryption based on a magic matrix with authentication ability is proposed. The proposed scheme applies XOR to encrypt the un-authorized and sensitive regions in the first layer of encryption. After using the magic matrix, the second layer of encryption is applied to encrypt the whole image. Moreover, the authentication was integrated into the image encryption scheme to authenticate whether the decrypted image is a fake one or not. The promising experiments have demonstrated the feasibility of the proposed scheme. In the next phase, the authors will explore other possible permutations of encryption methods to

further extend applicability to other smart living scenarios, such as IoT-enabled applications with security enhancement.



(a) Lena (b) FLE of Lena

(c) SLE of Lena (d) DR of image (c)

(e) Baboon (f) FLE of Baboon

(g) SLE of Baboon (h) DR of image (g)

Fig. 4. Results of image encryption and decryption.

ACKNOWLEDGMENT

Many thanks for the support by Ministry of Science and Technology in Taiwan under Grants MOST 104-2221-E-468-005, and MOST 104-2221-E-011-175, as well as from NTUST or Taiwan Tech) under Grants 104H230014, 104H451714, 104H210006, and 104H410306.

REFERENCES

[1] J. M. Barton, "Method and Apparatus for Embedding Authentication Information within Digital Data," United States Patent #5646997, Issued Jul. 8, 1997.

[2] E. Bertino, S. Castano and E. Ferrar, "Securing XML Documents with Author-X," *IEEE Internet Computing*, vol. 5**,** no. 3, pp. 21–31, 2001.

[3] R. Chand and P. Felber, "Scalable Distribution of XML Content with XNET," *IEEE Transactions on Parallel and Distributed Systems*, vol. 19, no. 4, pp. 447-461, 2008.

[4] Y. H. Chen, E. J. L. Lu, and P. J. Chen, "Fine-Grained Access Control for Digital Image Systems," *2014 International Conference on Information Science, Electronics and Electronical Engineering* (ISEEE2014), Sapporo, Japan, 2014.

[5] E. Damiani, S. D. C. d. Vimercati, S. Paraboschi and P. Samarati, "A Fine-grained Access Control System for XML Documents," *ACM Transactions on Information and System Security*, vol. 5, no. 2**,** pp. 169–202, 2002.

[6] R. Grosbois, P. Gerbelot and T. Ebrahimi, "Authentication and Access Control in The JPEG 2000 Compressed Domain," *SPIE Proc. of 46th Annual Meeting Applications of Digital Image Processing XXIV*, San Diego, 95-104, 2001.

[7] W. Hong, T. S. Chen, and H. Y. Wu, "An Improved Reversible Data Hiding in Encrypted Images Using Side Match," *IEEE Signal Processing Letters*, vol. 19, no. 4, pp. 199-202, 2012.

[8] Y. Hu, H. K. Lee, and J. Li, "DE-based Reversible Data Hiding with Improved Overflow Location Map," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 2, pp. 250-260, 2009.

[9] S. Imaizumi, O. Watanabe, M. Fujiyoshi, H. Kiya, "Generalized Hierarchical Encryption of JPEG 2000 Code Streams for Access Control," *IEEE Proc. of Conf. On Image Processing*, Genoa, Italy, pp. 1094-1097, 2005.

[10] N. Li, Q. Wang, W. Qardaji, E. Bertino, P. Rao, J. Lobo and D. Lin, "Access Control Policy Combining: Theory Meets Practice," *Proceedings of the 14th ACM symposium on Access control models and technologies*, pp. 135-144, 2010.

[11] C. C. Lin, Y. H. Chen and C. C. Chang, "LSB-based High-Capacity Data Embedding Scheme for Images," *International Journal of Innovational Computing and Information Control (IJICIC)*, Vol. 5, No. 11(B), pp. 4283-4289, 2009.

[12] E. J. L. Lu and Y. H. Chen, "A Flexible Delegation Processor for Web-based Information Systems," *Computer Standards and Interfaces*, vol. 27, no. 3, pp. 241-256, 2005.

[13] Q. Ni, E. Bertino, C. Brodie, C. M. Karat, J. Karat, J. Lobo and A. Trombetta, "Privacy-aware Role-based Access Control," *ACM Transactions on Information and System Security (TISSEC)*, vol. 13, no. 3, pp. 35-43, 2010.

[14] M. Pickering, L.E. Coria, P. Nasiopoulos, "A Novel Blind Video Watermarking Scheme for Access Control Using Complex Wavelets", *IEEE Proc. of Conf. on Consumer Electronics*, Las Vegas, NV, pp. 1-2, 2007.

[15] A. Phadikar, M.K. Kundu, S.P. Maity, "Quality Access Control of A Compressed Gray Scale Image," *Proc. of Conf. On*

Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG 08), India, pp. 13-19, 2008.

[16] X. Zhang, "Reversible Data Hiding in Encrypted Image," *IEEE Signal Processing Letters,* vol. 18, no. 4, pp. 255-258, 2011.

[17] X. Zhang, "Separable Reversible Data Hiding in Encrypted Image," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826-832, 2012.