

ISSN 2313-1527 (PRINT)  
ISSN 2313-1535 (ONLINE)

# IJEIE

*International Journal of Electronics  
and Information Engineering*

Vol. 5, No. 1 (Sept. 2016)

## Editor-in-Chief

**Prof. Min-Shiang Hwang**

Department of Computer Science & Information Engineering, Asia University, Taiwan

## Publishing Editors

**Candy C. H. Lin**

## Board of Editors

---

**Saud Althuniba**

Department of Communications Engineering of Al-Hussein Bin Talal University (Jordan)

**Jafar Ahmad Abed Alzubi**

College of Engineering, Al-Balqa Applied University (Jordan)

**Majid Bayat**

Department of Mathematical Sciences and Computer, University of Kharazmi (Iran)

**Yu Bi**

University of Central Florida (USA)

**Mei-Juan Chen**

National Dong Hwa University (Taiwan)

**Chen-Yang Cheng**

National Taipei University of Technology (Taiwan)

**Yung-Chen Chou**

Department of Computer Science and Information Engineering, Asia University (Taiwan)

**Christos Chrysoulas**

University of Patras (Greece)

**Christo Dichev**

Winston-Salem State University (USA)

**Xuedong Dong**

College of Information Engineering, Dalian University (China)

**Mohammad GhasemiGol**

University of Birjand (Iran)

**Dariusz Jacek Jakobczak**

Department of Electronics and Computer Science, Koszalin University of Technology (Poland)

**N. Muthu Kumaran**

Electronics and Communication Engineering, Francis Xavier Engineering College (India)

**Andrew Kusiak**

Department of Mechanical and Industrial Engineering, The University of Iowa (USA)

**John C.S. Lui**

Department of Computer Science & Engineering, Chinese University of Hong Kong (Hong Kong)

**Gregorio Martinez**

University of Murcia (UMU) (Spain)

**Sabah M.A. Mohammed**

Department of Computer Science, Lakehead University (Canada)

**Lakshmi Narasimhan**

School of Electrical Engineering and Computer Science, University of Newcastle (Australia)

**Khaled E. A. Negm**

Etisalat University College (United Arab Emirates)

**S. R. Boselin Prabhu**

SVS College of Engineering (India)

**Antonio Pescapè**

University of Napoli "Federico II" (Italy)

**Rasoul Ramezani**

Sharif University of Technology (Iran)

**Hemraj Saini**

Jaypee University of Information Technology (India)

**Michael Sheng**

The University of Adelaide (Australia)

**Yuriy S. Shmaliy**

Electronics Engineering, Universidad de Guanajuato (Mexico)

**Tony Thomas**

School of Computer Engineering, Nanyang Technological University (Singapore)

**Mohsen Toorani**

Department of Informatics, University of Bergen (Norway)

**Chia-Chun Wu**

Department of Industrial Engineering and Management, National Quemoy University (Taiwan)

**Nan-I Wu**

Toko University (Taiwan)

**Cheng-Ying Yang**

Department of Computer Science, University of Taipei (Taiwan)

**Chou-Chen Yang**

Department of Management of Information Systems, National Chung Hsing University (Taiwan)

**Sherali Zeadally**

Department of Computer Science and Information Technology, University of the District of Columbia (USA)

**Jianping Zeng**

School of Computer Science, Fudan University (China)

**Justin Zhan**

School of Information Technology & Engineering, University of Ottawa (Canada)

**Yan Zhang**

Wireless Communications Laboratory, NICT (Singapore)

## PUBLISHING OFFICE

**Min-Shiang Hwang**

Department of Computer Science & Information Engineering, Asia University, Taichung 41354, Taiwan, R.O.C.

Email: [mshwang@asia.edu.tw](mailto:mshwang@asia.edu.tw)

International Journal of Electronics and Information Engineering is published both in traditional paper form (ISSN 2313-1527) and in Internet (ISSN 2313-1535) at <http://ijeie.jalaxy.com.tw>

**PUBLISHER: Candy C. H. Lin**

© Jalaxy Technology Co., Ltd., Taiwan 2005

23-75, P.O. Box, Taichung, Taiwan 40199, R.O.C.

# International Journal of Electronics and Information Engineering

**Vol. 5, No. 1 (Sept. 1, 2016)**

1. Analysis of Two Confidentiality-Preserving Image Search Schemes Based on Additive Homomorphic Encryption  
Lihua Liu, Zhengjun Cao 1-5
2. Dual Image Based Reversible Data Hiding Scheme Using Weighted Matrix  
Biswapati Jana 6-19
3. The Encryption Algorithm AES-RFWKPES32-4  
Aripov Mirsaid, Tuychiev Gulom 20-29
4. A Note on Efficient Algorithms for Secure Outsourcing of Bilinear Pairings  
Lihua Liu and Zhengjun Cao 30-36
5. Pixel Value Differencing Method Based on CMYK Colour Model  
Shobana Manoharan, Deepika RajKumar 37-46
6. Selecting Internet Videos and Pictures for Personalized Reminiscence Therapy  
Hui-Wen Chien, Shu-Chuan Liao, Song-Lin Huang, Ching-Mao Chang, Hui-Ling Chen and Hsueh-Ting Chu 47-55



# Analysis of Two Confidentiality-Preserving Image Search Schemes Based on Additive Homomorphic Encryption

Lihua Liu<sup>1</sup> and Zhengjun Cao<sup>2</sup>

(Corresponding author: Zhengjun Cao)

Department of Mathematics, Shanghai Maritime University<sup>1</sup>  
No.1550, Haigang Ave, Pudong New District, Shanghai, China

Department of Mathematics, Shanghai University<sup>2</sup>  
No.99, Shangda Road, Shanghai, 200444, China

(Email: caozhj@shu.edu.cn)

(Received May 14, 2016; revised and accepted July 20, 2016)

## Abstract

Recently, Lu et al. have proposed two image search schemes based on additive homomorphic encryption [IEEE Access, 2 (2014), 125-141]. We remark that both schemes are flawed because: (i) the first scheme does not make use of the additive homomorphic property at all; (ii) the additive homomorphic encryption in the second scheme is unnecessary and can be replaced by a more efficient symmetric key encryption.

*Keywords:* Additive Homomorphic Encryption; Confidentiality-preserving Image Search; Symmetric Key Encryption

## 1 Introduction

Homomorphic encryption, introduced by Rivest, Adleman and Dertouzos [14], is a useful primitive since it can translate an operation on the ciphertexts into an operation on the corresponding plaintexts. The property is very appreciated for some applications, such as e-voting, watermarking and secret sharing schemes. For example, if an additively homomorphic encryption is used in an e-voting scheme, one can obtain an encryption of the sum of all ballots from their encryption. Consequently, a single decryption will reveal the result of the election.

In 1999, Paillier [13] put forth a public-key cryptosystem which encrypts a message  $m$  by  $E(m, r) = g^m r^n \bmod n^2$ , where  $n = pq$  is an RSA modulus,  $g$  is a public parameter such that  $n \mid \text{ord}_{n^2}(g)$ , and  $r$  is a random pad. The function  $E(m, r)$  has the additively homomorphic property:  $E(m_1, r_1)E(m_2, r_2) = E(m_1 + m_2, r_1 r_2)$ . At PKC'01, Damgård and Jurik [6] proposed a generalization of Paillier's encryption using modulo  $n^i (i \geq 2)$ . The elliptic curve variant of Paillier's cryptosystem is due to Galbraith [7]. In 2001, Choi et al. [5] revisited the Paillier's encryption by taking a special base. At Eurocrypt'06, Schoenmakers and Tuyls [15] considered that converting a given Paillier's encryption of a value  $x \in \mathbb{Z}_n$  into Paillier's encryption of the bits of  $x$ . At Eurocrypt'13, Joye and Libert [9] obtained another generalization of Paillier's encryption.

In 2013, Boneh et al. [1] considered private database queries using Paillier's encryption. At Asiacrypt' 14, Catalano et al. [3] presented an instantiation of publicly verifiable delegation of computation on outsourced ciphertext which supports Paillier's encryption. To this day, Paillier's cryptosystem is still more competitive for applications that need only to add ciphertexts. Recently, Hsien et al. have investigated the possible usage of homomorphic encryption in client-server scenario [2, 4, 8, 10, 11].

Very recently, Lu et al. [12] have discussed how existing additive homomorphic encryption can be potentially used for image search, and proposed two confidentiality-preserving image search schemes based on Paillier's encryption. In the proposed model, a client has many images and wants to store the image data online for convenient data access anywhere anytime. The client has to encrypt each image and its features and upload the encrypted data to a cloud server.

In this note, we remark that both Lu et al.'s schemes are flawed. The first scheme does not make use of the additive homomorphic property at all. The additive homomorphic encryption in the second scheme is unnecessary and can be reasonably replaced by a more efficient symmetric key encryption such as AES.

Table 1: Lu et al.'s Scheme 1

Client	Server
Encrypt the image $P^{(i)}$ and its feature vector $\mathbf{f}^{(i)} \in \mathbb{R}^t$ as $\mathcal{E}(\mathbf{f}^{(i)}) = (\mathcal{E}(f_1^{(i)}), \dots, \mathcal{E}(f_t^{(i)}))$ and $E(P^{(i)})$ . Upload them.	Store the encrypted images and features.
Given an image $Q$ and its feature vector $\mathbf{q}$ , ask for all the encrypted features.	$\xrightarrow{\text{Request}}$ $\xleftarrow[\substack{i=1, \dots, N}]{\{i, \mathcal{E}(\mathbf{f}^{(i)})\}}$ Return all encrypted features.
Compute $\mathbf{f}^{(i)} = \mathcal{D}(\mathcal{E}(\mathbf{f}^{(i)}))$ and the $L_2$ distance $d_i = \ \mathbf{f}^{(i)} - \mathbf{q}\ $ , $i = 1, \dots, N$ . Send $\mathcal{I} = \{j \mid d_j \leq \lambda\}$ , where $\lambda$ is a fault-tolerant parameter.	$\xrightarrow{\mathcal{I}}$ $\xleftarrow[\substack{k \in \mathcal{I}}]{\{E(P^{(k)})\}}$ Return all $E(P^{(k)}), k \in \mathcal{I}$ .
Recover all $P^{(k)} = \mathcal{D}(E(P^{(k)})), k \in \mathcal{I}$ .	

## 2 Review of Lu et al.'s Schemes

In the schemes [12], the features of each image are encrypted by any additively homomorphic encryption such as Paillier's cryptosystem [13], which can be described as follows. Pick an RSA modulus  $n = pq$ . Set  $\lambda = \text{lcm}(p-1, q-1)$ . Select  $g \in \mathbb{Z}_{n^2}^*$  such that  $n \mid \text{ord}_{n^2}(g)$ .

Publish  $n, g$  and keep  $\lambda$  in secret. For  $m \in \mathbb{Z}_n$ , pick  $r \in \mathbb{Z}_n$ , compute the ciphertext  $c = \mathcal{E}(m) = g^m r^n \bmod n^2$ . Recover  $m = \mathcal{D}(c) = \left( \frac{c^\lambda - 1 \bmod n^2}{n} \right) / \left( \frac{g^\lambda - 1 \bmod n^2}{n} \right) \bmod n$ .

Denote the encrypting function and decrypting function of AES by  $E(\cdot)$  and  $D(\cdot)$ , and that of Paillier's cryptosystem by  $\mathcal{E}(\cdot)$  and  $\mathcal{D}(\cdot)$ , respectively. See Table 1 and Table 2 for the details of the two image search schemes.

Notice that by the additive homomorphic property of Paillier's encryption, we have

$$\begin{aligned}
 \mathcal{E}(\|\mathbf{f}^{(i)} - \mathbf{q}\|^2) &= \mathcal{E}\left(\sum_{\ell=1}^t (f_\ell^{(i)} - q_\ell)^2\right) \\
 &= \mathcal{E}\left(\sum_{\ell=1}^t (f_\ell^{(i)})^2 - 2\sum_{\ell=1}^t f_\ell^{(i)} q_\ell + \sum_{\ell=1}^t q_\ell^2\right) \\
 &= \mathcal{E}\left(\sum_{\ell=1}^t (f_\ell^{(i)})^2\right) \cdot \mathcal{E}\left(-2\sum_{\ell=1}^t f_\ell^{(i)} q_\ell\right) \cdot \mathcal{E}\left(\sum_{\ell=1}^t q_\ell^2\right) \\
 &= \chi_i \cdot \left(\prod_{\ell=1}^t (\mathcal{E}(f_\ell^{(i)}))^{q_\ell}\right)^{-2} \cdot \mathcal{E}\left(\sum_{\ell=1}^t q_\ell^2\right) \\
 &= h_i, \\
 d_i &= \mathcal{D}(h_i) = \mathcal{D}\left(\mathcal{E}(\|\mathbf{f}^{(i)} - \mathbf{q}\|^2)\right) = \|\mathbf{f}^{(i)} - \mathbf{q}\|^2.
 \end{aligned}$$

## 3 Analysis of Lu et al.'s Schemes

We now show that Lu et al.'s schemes are flawed.

- 1) The authors [12] have *confused the general arithmetic over the field  $\mathbb{R}$  and the modular arithmetic over the domain  $\mathbb{Z}_n$* . In fact, the correctness of the schemes are based on

$$\mathbf{f}^{(i)} = \mathcal{D}(\mathcal{E}(\mathbf{f}^{(i)})), \quad \|\mathbf{f}^{(i)} - \mathbf{q}\|^2 = \mathcal{D}\left(\mathcal{E}(\|\mathbf{f}^{(i)} - \mathbf{q}\|^2)\right).$$

Table 2: Lu et al.'s Scheme 2

Client	Server
Encrypt the image $P^{(i)}$ and its feature vector $\mathbf{f}^{(i)} \in \mathbb{R}^t$ as $\mathcal{E}(\mathbf{f}^{(i)}) = (\mathcal{E}(f_1^{(i)}), \dots, \mathcal{E}(f_t^{(i)}))$ and $E(P^{(i)})$ . Compute $\chi_i = \mathcal{E}\left(\sum_{\ell=1}^t (f_\ell^{(i)})^2\right)$ .	$\xrightarrow[i=1, \dots, N]{\{i, \chi_i, \mathcal{E}(\mathbf{f}^{(i)}), E(P^{(i)})\}}$ Store the encrypted images.
Given an image $Q$ and its feature vector $\mathbf{q}$ , send $\mathbf{q}$ to the server. Compute $d_i = \mathcal{D}(h_i)$ , $i = 1, \dots, N$ . Randomly pick a set $\widehat{\mathcal{I}} \subset \{1, \dots, N\}$ of an appropriate size. Set $\mathcal{I}' = \widehat{\mathcal{I}} \cup \mathcal{I}$ where $\mathcal{I} = \{j \mid d_j \leq \lambda, 1 \leq j \leq N\}$ , $\lambda$ is a fault-tolerant parameter. Recover all images $P^{(k)} = D(E(P^{(k)})), k \in \mathcal{I}$ .	$\xrightarrow{\mathbf{q}}$ Compute $h_i = \left(\prod_{\ell=1}^t (\mathcal{E}(f_\ell^{(i)}))^{q_\ell}\right)^{-2} \cdot \mathcal{E}\left(\sum_{\ell=1}^t q_\ell^2\right) \cdot \chi_i, i = 1, \dots, N$ . $\xleftarrow[h_i, i=1, \dots, N]{\mathcal{I}'}$ Return all $E(P^{(k)}), k \in \mathcal{I}'$ . $\xleftarrow[k \in \mathcal{I}']{\{E(P^{(k)})\}}$

Table 3: The revised version of Lu et al.'s Scheme 1

Client	Server
Encrypt the image $P^{(i)}$ and its feature vector $\mathbf{f}^{(i)} \in \mathbb{Z}_n^t$ as $E(\mathbf{f}^{(i)}) = (E(f_1^{(i)}), \dots, E(f_t^{(i)}))$ and $E(P^{(i)})$ . Upload them.	$\xrightarrow[i=1, \dots, N]{\{i, E(\mathbf{f}^{(i)}), E(P^{(i)})\}}$ Store the encrypted images and features.
Given an image $Q$ and its feature vector $\mathbf{q}$ , ask for all the encrypted features. Compute $\mathbf{f}^{(i)} = D(E(\mathbf{f}^{(i)}))$ and the $L_2$ distance $d_i = \ \mathbf{f}^{(i)} - \mathbf{q}\ $ for all $i = 1, \dots, N$ . Send $\mathcal{I} = \{j \mid d_j \leq \lambda\}$ , where $\lambda$ is a fault-tolerant parameter. Recover all images $P^{(k)} = D(E(P^{(k)})), k \in \mathcal{I}$ .	Upon receiving the request, send all encrypted features back. $\xleftarrow[h_i, i=1, \dots, N]{\{i, E(\mathbf{f}^{(i)})\}}$ $\xrightarrow{\mathcal{I}}$ Return all the encrypted images $E(P^{(k)}), k \in \mathcal{I}$ . $\xleftarrow[k \in \mathcal{I}]{E(P^{(k)})}$

Table 4: Dominated computations for the client in three schemes

	Dominated computations	Computational cost
Scheme 1	$\mathbf{f}^{(i)} = \left( \mathcal{D}(\mathcal{E}(f_1^{(i)})), \dots, \mathcal{D}(\mathcal{E}(f_t^{(i)})) \right),$ $i = 1, \dots, N.$ $P^{(k)} = D(E(P^{(k)})), k \in \mathcal{I}.$	public key decryption: $tN$ (times) symmetric key decryption: $ \mathcal{I} $
Scheme 2	$d_i = \mathcal{D}(h_i), i = 1, \dots, N.$ $P^{(k)} = D(E(P^{(k)})), k \in \mathcal{I}.$	public key decryption: $N$ symmetric key decryption: $ \mathcal{I} $
The revised	$\mathbf{f}^{(i)} = D(E(\mathbf{f}^{(i)})), i = 1, \dots, N.$ $P^{(k)} = D(E(P^{(k)})), k \in \mathcal{I}.$	symmetric key decryption: $N +  \mathcal{I} $

The equations hold on the condition that  $\mathbf{f}^{(i)}$  and  $\|\mathbf{f}^{(i)} - \mathbf{q}\|^2$  are in the underlying domain  $\mathbb{Z}_n$  of Paillier's encryption. That means a visual feature vector  $\mathbf{f} \in \mathbb{R}^t$  must be transformed into  $\mathbf{f} \in \mathbb{Z}_n^t$ . But the authors [12] have not specified this process.

- 2) In the scheme 1, both the client and the server do not make use of the additive homomorphic property of Paillier's encryption at all. The related computations for the client are

$$\mathbf{f}^{(i)} = \mathcal{D}(\mathcal{E}(\mathbf{f}^{(i)})), i = 1, \dots, N.$$

Actually, the process has no relation to the additive homomorphic property. Thus, the Paillier's public key encryption in the scheme can be reasonably replaced by the more efficient symmetric key encryption AES.

It seems that the authors have not realized that the computational performance of public-key encryption is inferior to that of symmetric-key encryption. For example, the authors wrote [12] "image encryption can be done using state-of-the-art ciphers such as AES or RSA by treating images as ordinary data". We here would like to stress that images should be encrypted by a symmetric key encryption, instead of any public key encryption. In practice, RSA is usually used for encrypting session keys, not for images. Compared with AES, RSA is fairly inefficient.

- 3) In Scheme 2, the server has to make use of the additive homomorphic property for computing the encrypted distance  $h_i = \mathcal{E}(\|\mathbf{f}^{(i)} - \mathbf{q}\|^2)$ . But in such case, the client has still to compute  $d_i = \mathcal{D}(h_i), i = 1, \dots, N$ , which dominate the client's computational cost. Compared with the revised scheme (see Table 3 for the revised version of the scheme 1.), we find, Scheme 2 has not truly mitigated the client's computational cost. See Table 4 for the comparisons of the dominated computations for the client in three schemes. Apparently, the revised scheme is more efficient because it only needs to perform symmetric key decryption  $N + |\mathcal{I}|$  times.

## 4 Conclusion

We would like to stress that the computational performance of public-key encryption is inferior to that of symmetric-key encryption. A homomorphic encryption allows anyone to perform some computations on encrypted data, despite not having the secret decryption key. But any computations performed on encrypted data are constrained to the underlying domain (finite domains). This restriction makes the primitive useless for most computations involving common arithmetic expressions and relational expressions. We stress that the real goal of using modular arithmetic in cryptography is to obscure and dissipate the redundancies in a plaintext message, not to perform any numerical calculations.

## Acknowledgments

The authors would like to thank the National Natural Science Foundation of China (Project 61303200, 61411146001). The authors gratefully acknowledge the reviewers for their valuable suggestions.



## References

- [1] D. Boneh, C. Craigentry, S. Halevi, F. Wang, and D. Wu, "Private database queries using somewhat homomorphic encryption," in *Proceedings of Applied Cryptography and Network Security (ACNS'13)*, pp. 102–118, Banff, AB, Canada, June 2013.
- [2] Z. J. Cao and L. H. Liu, "The paillier's cryptosystem and some variants revisited," *International Journal of Network Security*, vol. 19, no. 1, pp. 89–96, 2017.
- [3] D. Catalano, A. Marcedone, and O. Puglisi, "Authenticating computation on groups: New homomorphic primitives and applications," in *Proceedings of Advances in Cryptology - ASIACRYPT 2014*, pp. 193–212, Kaoshiung, Taiwan, R.O.C., Dec. 2014.
- [4] T. Y. Chen, C. C. Lee, M. S. Hwang, and J. K. Jan, "Towards secure and efficient user authentication scheme using smart card for multi-server environments," *Journal of Supercomputing*, vol. 66, no. 2, pp. 1008–1032, 2013.
- [5] D. Choi, S. Choi, and D. Won, "Paillier's cryptosystem revisited," in *Proceedings of 8th ACM Conference on Computer and Communications Security (CCS'01)*, pp. 206–214, Philadelphia, Pennsylvania, USA, Nov. 2001.
- [6] I. Damgård and J. Jurik, "A generalisation, a simplification and some applications of paillier's probabilistic public-key system," in *Proceedings of Public Key Cryptography (PKC'01)*, pp. 119–136, Cheju Island, Korea, Feb. 2001.
- [7] D. Galbraith, "Elliptic curve paillier schemes," *Journal of Cryptology*, vol. 15, no. 2, pp. 129–138, 2002.
- [8] W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133–142, 2016.
- [9] M. Joye and B. Libert, "Efficient cryptosystems from 2k-th power residue symbols," in *Proceedings of Advances in Cryptology (EUROCRYPT'13)*, pp. 76–92, Athens, Greece, May 2013.
- [10] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of attribute-based access control with user revocation in cloud data storage," *International Journal of Network Security*, vol. 18, no. 5, pp. 900–916, 2016.
- [11] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing," *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.
- [12] W. Lu, A. L. Varna, and M. Wu, "Confidentiality-preserving image search: A comparative study between homomorphic encryption and distance-preserving randomization," *IEEE Access*, no. 2, pp. 125–141, 2014.
- [13] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proceedings of Advances in Cryptology (EUROCRYPT'99)*, pp. 223–238, Prague, Czech Republic, May 1999.
- [14] R. Rivest, L. Adleman, and M. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of Secure Computation*, pp. 169–180, 1978.
- [15] B. Schoenmakers and P. Tuyls, "Efficient binary conversion for paillier encrypted values," in *Proceedings of Advances in Cryptology (EUROCRYPT'06)*, pp. 522–537, St. Petersburg, Russia, May 2006.

## Biography

**Lihua Liu** is an associate professor of Department of Mathematics at Shanghai Maritime University. She received her Ph.D. degree in applied mathematics from Shanghai Jiao Tong University. Her research interests include combinatorics, cryptography and information security.

**Zhengjun Cao** is an associate professor of Department of Mathematics at Shanghai University. He received his Ph.D. degree in applied mathematics from Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He served as a post-doctor in Computer Sciences Department, Université Libre de Bruxelles, from 2008 to 2010. His research interests include cryptography, discrete logarithms and quantum computation.

# Dual Image Based Reversible Data Hiding Scheme Using Weighted Matrix

Biswapati Jana

Department of Computer Science, Vidyasagar University

Midnapore, Pin-721102, India

(E-mail: biswapatijana@gmail.com)

(Received Sept. 9, 2015; revised and accepted May 12 & Aug. 1, 2016)

## Abstract

In this paper, we introduce dual image based reversible data hiding scheme using weighted matrix. First, we partition the original image into  $(3 \times 3)$  pixel blocks. Then we perform modulo sum of entry wise multiplication with a shared secret weighted matrix. We then calculate the difference between modulo sum value and secret message. According to the sign of this difference, we increase or decrease one at the corresponding pixel of image block and keep the position value by addition/subtraction with the original pixel. Repeat the same nine times to embed thirty six bits secret data within each pixel block. Finally, we distribute the original and stego pixel among dual image based on a shared secret key. At the receiver end, we successfully extract secret message using shared secret weighted matrix and shared secret key. Also we recover cover image without any distortion from dual stego image as because the original pixels are not effected during data embedding which assure reversibility. The proposed scheme provides average data embedding capacity 1.98 bits per pixel (bpp) with good visual quality measured by peak signal to noise ratio (PSNR) which are grater than 39 dB. We compare our scheme with other state-of-the-art methods and obtain reasonably better performance in terms of data embedding capacity.

*Keywords: Dual Image; Reversible Data Hiding; RS Analysis; Steganographic Attack; Weighted Matrix*

## 1 Introduction

The data hiding is a form of covered communication that usually puts stress on simply finding the presence of a secret message. The main intention of hidden data communication is to concentrate on precluding the adversary from moving out the content of the confidential message by applying a variety of distortions techniques. Thus, the imperceptibility becomes the most significant place for the data hiding schemes. A high embedding efficiency becomes the principal aim to accomplish for the current data hiding schemes by substituting the payload. Westfeld [27] proposed F5 algorithm that is an good example of this kind of scheme. In this scheme, matrix embedding is used based on Hamming codes to embed  $k$ -bits secret data by changing least significant bit in the cover work. The embedding efficiency gains with the increment of  $k$ , while the payload falls contrarily. In order to enhancing the embedding efficiency and payload at the same time, an extended F5 algorithm is proposed by Fan et al. [8]. A data hiding scheme for binary images, which uses a binary matrix and a weight matrix to enforce insertion, is mentioned by Tseng [23]. However, the embedding efficiency and payload cannot reach the best level when the scheme is used to deal with gray-scale image. Also the scheme was not reversible. Here, we propose high embedding reversible data hiding scheme using weighted matrix through dual image. In addition, a high-risk security vulnerability is exist because an attacker will be able to guess the form of weight matrix by using brute-force attack. In order to overcome the drawbacks of the previous schemes [8, 23], an improved embedding strategy is developed in this paper. We introduce shared secret key  $\xi$  to enhance the security and update weighted matrix for every new block by  $W_{i+1} = (W_i \times \kappa - 1) \bmod 9$ , where  $\gcd(\kappa, 9) = 1$ . The secret key  $\xi$  is required to distribute the updated pixel among dual image. The proposed scheme improve the embedding capacity and achieve reversibility.

### 1.1 Motivation

In this paper, we introduce a new dual image based reversible data hiding scheme using weighted matrix.

- Our main motivation is to enhance the embedding capacity, security and to achieve reversibility in data hiding. Data embedding schemes using weighted matrix was not reversible. We develop dual image based reversible data hiding scheme using weighted matrix.

- To enhance security we update weighted matrix for each new block. It is possible by using the update rule  $W_{i+1} = (W_i \times \kappa - 1) \bmod 9$ , where  $\gcd(\kappa, 9) = 1$ . Also, we use a shared secret key bit stream  $\xi$  to distribute original pixel and stego pixel among dual image.
- To enhance capacity, we use nine times modulo sum of entry wise multiplication with each block. In Li Fan et al.'s [7] scheme, only single sum of entry-wise multiplication is applied on single block of cover image. Here, we enhance the embedding capacity through weight matrix based data hiding scheme, where we can hide thirty six secret data bits within each block of cover image using dual image. As a result, In a  $(256 \times 256)$  cover image, we can hide more than 2,60,100 bits. So, the payload is 1.98 bpp.
- To achieve reversibility in weighted matrix, we use dual image where stego pixel and original pixel are distribute among dual image and we can find the original pixel depending on the shared secret key bit stream  $\xi$ .

The rest of the paper is organized as follows. Section 2 describes literature review. Proposed data hiding scheme are discussed in Section 3. Experimental results with comparisons are discussed in Section 4. The steganographic security analysis are given in Section 5 and steganographic attacks are presented in Section 6. Finally, conclusions are given in Section 7.

## 2 Literature Review

The modern secret writings are tweaked the cover work in such a way that a secret message can be encoded within them. The secret message insertion may change every bit of information in the cover data. There are a number of ways to conceal information within the cover work. The most usual methodologies are based on the least significant bits (LSBs) substitution [2, 4, 25] and the modulus operation [3, 22, 26]. Reversible data hiding using block is commonly used to increase visual quality or to achieve reversibility [13, 14, 17, 19, 28]. Reversible data hiding (RDH) presented by Ni et al. [18] is based on histogram shifting with zero or minimum change of the pixel gray values. Multilevel reversible data hiding based on histogram shifting is proposed by Lin et al. [15] and Tsai et al. [24]. Adaptive reversible data hiding method using integer transform is presented by Peng et al. [20]. Designing a novel data hiding system accomplishing good visual quality, high embedding capacity, robustness and steganographic protection is a technically challenging problem. Chang et al. [5] proposed a reversible data hiding scheme using two steganographic images. Lee et al. [12] developed a reversible data hiding scheme using dual stego-images, in which only one pixel value needs to be modified by at most plus or minus 1 for carrying two-bit data. Lee and Huang [11] developed a dual-image based reversible data hiding method that overcomes the drawbacks of the above methods. A secure data hiding scheme for binary images using a key matrix and a weight matrix  $W$  has been proposed by Tseng et al. [23] which can hide only 2 bits in a  $(3 \times 3)$  block of pixels. Li Fan et al. [7] proposed an improved efficient data hiding scheme using weight matrix for gray scale images which can hide 4 bits in a  $(3 \times 3)$  block. In both the matrix based schemes, only one modular sum of entry wise multiplication of weighted matrix  $W$  is performed with a  $(3 \times 3)$  block of pixel in the original image. Only one embedding operation is performed with a single block and only 4 bits data embed within the block. High-capacity is still one of important research issues in data hiding. After the confidential message is extracted, the requirement for the image reversibility for the entire recovery of the original object without any distortion goes high. Here, we propose a high capacity reversible data hiding scheme using dual image, where we can hide thirty six bits secret data in each block. The scheme achieves good PSNR and high payload.

## 3 Proposed Scheme

Consider the weighted matrix  $W$  of size  $(3 \times 3)$ . Then we perform modular sum of entry wise multiplication of original image block  $B_{3 \times 3}$  with weighted matrix  $W$ . We calculate data embedding position by subtracting the modular sum value  $v$  from secret data unit  $D = d_1, d_2, \dots$ , that is,  $p = d_i - v$ . We check the sign of calculated position value ( $p$ ). If the sign of  $p$  is positive/negative, then we increase/decrease the desired pixel value by one unit at the desired position of  $B_{(3 \times 3)}$  pixel block. At the same time, we store the embedding position that is  $p$  by adding/subtracting within dual image stego major (SM) and stego auxiliary (SA). We distribute original pixel (OP) in one image and create a new pixel (NP). We then store NP in another image. Each time one OP is increased or decreased by  $p$  to generate the NP. Increase (or decrease) operation says the  $d$  value either 1 (or  $-1$ ). SM or SA holds OP or NP decided by  $\xi_{(\bmod(j, \text{length}(\xi)) + 1)}$ . Since  $\xi$  is the key in binary form,  $\bmod(j, \text{length}(\xi)) + 1$  indicates the index value where  $j=1, 2, 3, \dots$ . If  $\xi_{(\bmod(j, \text{length}(\xi)) + 1)} = 1$  then OP is stored in SM and NP is stored in SA; otherwise, OP is stored in SA and NP is stored in SM. After the block  $I_i$  completely examined,  $W$  is modified by Equation (1)

$$W_{i+1} = (W_i \times \kappa - 1) \bmod 9, \text{ where } \gcd(\kappa, 9) = 1 \quad (1)$$

When all data are examined, then process will be stopped and finally two stego images  $SM$  and  $SA$  are produced.  $\xi$ ,  $W$  and  $\kappa$  play an important role for data embedding and extraction.  $\xi$  is used for shuffling two modified pixels among dual image. The corresponding algorithm is described in Algorithm 1. The numerical illustration are shown in Figure 1.

---

**Algorithm 1 Data embedding**


---

**Input:** Cover Image ( $I_{m \times n}$ ), Weight matrix ( $W_{3 \times 3}$ ), Data  $D=d_1, d_2, d_3, \dots$ , where  $d_i = r$  bits each, Shared secret key  $\xi$  of 128 bits.

**Output:** Two stego image  $SM_{m \times n}$  and  $SA_{m \times n}$ ;

---

```

1: Initialize: Dcount=Kcount=1; sq=3; SM=I; SA=I;
2: for (s=1) to (m/sq) do
3:   for t=1 to (n/sq) do
4:      $B_{st}(3 \times 3) \leftarrow I_{m \times n}$ ;
5:     for i=(sq*(s-1))+1 to (sq*s) do
6:       for j=(sq*(t-1))+1 to (sq*t) do
7:          $SUM = B_{st} \otimes W_{st}$ ;
8:          $v = SUM \pmod{16}$ ;  $p=(d_{Dcount} - v)$ ;
9:         if ( $p > 0$ ) then
10:          if ( $p > 8$ ) then
11:             $p=(16-p)$ ;  $d=-1$ 
12:             $d=1$ ;
13:          end if
14:          if ( $p < -8$ ) then
15:             $p=abs(16+p)$ ;  $d=1$ 
16:             $p=abs(p)$ ;  $d=-1$ 
17:          end if
18:        end if
19:         $B_{st}(x, y) = B_{st}(x, y) + d$  if  $W_r(x, y)=p$ , where  $x=1,2,3$  and  $y=1,2,3$ ;
20:         $OP=I_{m \times n}(i, j)$ ;  $NP=I_{m \times n}(i, j) + (p \times d)$ ;
21:        if ( $\xi(Kcount) = 1$ ) then
22:           $SM_{m \times n}(i, j)=OP$ ;  $SA_{m \times n}(i, j)=NP$ ;
23:           $SM_{m \times n}(i, j)=NP$ ;  $SA_{m \times n}(i, j)=OP$ ;
24:          Dcount=Dcount+1; Kcount=Kcount+1;
25:          if (Kcount>length( $\xi$ )) then
26:            Kcount=1;
27:          end if
28:        end if
29:        if (Dcount>length(D)) then
30:          goto Line-37
31:        end if
32:      end for
33:    end for
34:     $W_{st+1} = ((W_{st} \times \kappa - 1) \pmod{9})$ , where  $\gcd(\kappa, 9) = 1$ ;
35:  end for
36: end for
37: Produce  $SM_{m \times n}$  and  $SA_{m \times n}$  stego image;

```

---

At the receiver end, data are extracted from stego image  $SM$  and  $SA$  using secret keys  $\xi$ ,  $\kappa$  and weighted matrix ( $W$ ). Using  $\xi$ , we first rearrange the original pixel ( $OP$ ) and new pixel ( $NP$ ) by selecting  $3 \times 3$  pixel block and generate the original image matrix ( $I$ ) and new image matrix ( $NM$ ) respectively. We generate a matrix ( $P\_MX$ ) of same size of  $I$  and  $NM$ .

$$P\_MX_{m \times n} = (I_{m \times n} - NM_{m \times n}) \quad (2)$$

The equation 2 is a simple matrix subtraction between  $I$  and  $NM$ . Now, we select each  $3 \times 3$  block from  $I_i$  for entry-wise-multiplication with  $W$ . Before multiplication  $I_i$  will be modified to  $I'_i$  by changing one pixel mentioned by  $P\_MX_i(x, y)$  where  $x = 1, 2, 3$  and  $y = 1, 2, 3$ . That means for value at  $P\_MX_i(1,1)$ ,  $I_i$  will be modified to  $I'_i$

by increasing or decreasing 1 to one pixel that depends on sign of the value of  $P\_MX_i(1,1)$ . After that sum of the entry-wise-multiplication will be calculated to get the  $r$  bits data over modulo  $2^r$ . Similarly for  $P\_MX_i(1,2)$ ,  $I'_i$  will be modified to  $I''_i$  and find the next  $r$  bits data. In this way, after 9 modification of  $I_i$  using  $P\_MX_i(3,3)$ , we modify  $W$ , then select  $I_{i+1}$  for next iteration. The algorithm of extraction procedure is shown in Algorithm-2. The numerical illustration is shown in Figure 2.

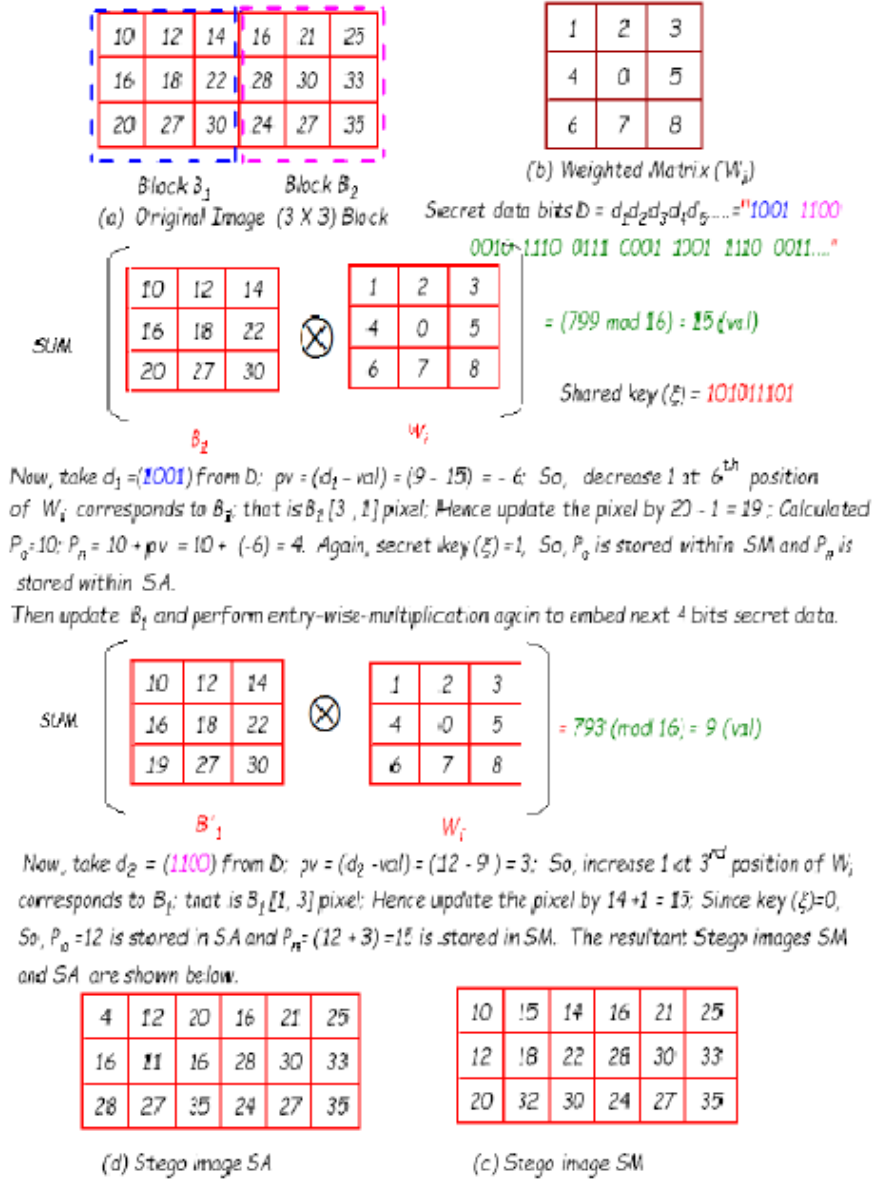


Figure 1: Example for data embedding

In this way hidden data  $D$  are extracted as well as original cover image is retrieved.

### 3.1 Overflow-Underflow Control

The  $p$  value is added or subtracted from  $OP$  to get  $NP$  and we put  $NP$  in one image and  $OP$  in other. So,  $OP$  is the original image and can not fall in overflow or underflow situation, but  $NP$  may fall. For example, if  $OP = 248$  and  $d = 1$ ,  $p$  value may be 8, then  $NP = (248 + 8) = 256$  which is greater than 255. So overflow situation will arise. Similarly, if  $OP = 6$  and  $d = -1$  and  $p = 7$ , then  $NP = (6 - 7) = -1$  which is less than 0. So underflow situation will arise.

**Algorithm 2** Data extraction

**Input:** Two stego image  $SM_{m \times n}$  and  $SA_{m \times n}$ ; Weight matrix( $W_{3 \times 3}$ ), shared secret key  $\xi$  of 128 bits;  $Dlen$  is the data length;

**Output:** Cover Image ( $I'_{m \times n}$ ), Data  $D' = \{d'_1, d'_2, d'_3, \dots, \text{where } d'_i = 4 \text{ bits each}\}$ ;

```

1: Initialize:  $Dcount = Kcount = 1$ ;  $sq = 3$ ;  $P\_MX$  is a matrix that hold the  $p$  value;  $I' = SM$ ;
2: for ( $s=1$  to  $(m/sq)$ ) do
3:   for ( $t=1$  to  $(n/sq)$ ) do
4:     for ( $i=(sq*(s-1))+1$  to  $(sq*s)$ ) do
5:       for ( $j=(sq*(t-1))+1$  to  $(sq*t)$ ) do
6:         if ( $\xi(Kcount) = 1$ ) then
7:            $OP = SM_{m \times n}(i, j)$ ;  $NP = SA_{m \times n}(i, j)$ ;  $I'_{st}(i, j)$ ;
8:         else
9:            $OP = SA_{m \times n}(i, j)$ ;  $NP = SM_{m \times n}(i, j)$ ;  $I'_{st}(i, j)$ ;
10:        end if
11:         $P\_MX_{st}(i, j) = (NP - OP)$ ;
12:      end for
13:       $Kcount = Kcount + 1$ ;
14:      if ( $Kcount > length(\xi)$ ) then
15:         $Kcount = 1$ ;
16:      end if
17:    end for
18:  end for
19: end for
20: for ( $s=1$  to  $(m/sq)$ ) do
21:   for ( $t=1$  to  $(n/sq)$ ) do
22:      $B_{st}(3 \times 3) \leftarrow I'_{m \times n}$ ;
23:     for ( $i=(sq*(s-1))+1$  to  $(sq*s)$ ) do
24:       for ( $j=(sq*(t-1))+1$  to  $(sq*t)$ ) do
25:         if ( $P\_MX_{st}(i, j) \neq 0$ ) then
26:            $p = P\_MX_{st}(i, j)$ ;  $d = 1$ ;
27:         end if
28:         if ( $P\_MX_{st}(i, j) \leq 0$ ) then
29:            $p = abs(P\_MX_{st}(i, j))$ ;  $d = -1$ ;
30:         end if
31:          $B_{st}(x, y) = B_{st}(x, y) + d$  if  $W_r(x, y) = p$ , where  $x=1, 2, 3$  and  $y=1, 2, 3$ ;
32:          $SUM = B_{st} \otimes W_{st}$ ;
33:         ( $d'_{Dcount} = SUM \pmod{16}$ );  $p = (d'_{Dcount} - v)$ ;
34:          $Dcount = Dcount + 1$ ;
35:         if ( $Dcount > Dlen$ ) then
36:           goto Line-43
37:         end if
38:       end for
39:     end for
40:      $W_{st+1} = ((W_{st} \times \kappa - 1) \pmod{9})$ , where  $\gcd(\kappa, 9) = 1$ ;
41:   end for
42: end for
43: Produce  $I'_{m \times n}$  and  $D' = \{d'_1, d'_2, d'_3, \dots, \text{where } d'_i = 4 \text{ bits each}\}$ 

```

To overcome this problem, we use equation 3. If  $OP$  is greater than 247 or less than 8 then  $NP$  is calculated by

$$NP = \begin{cases} 247 + (p \times d), & \text{if } OP > 247 \\ 8 + (p \times d), & \text{if } OP < 8 \\ OP + (p \times d), & \text{otherwise.} \end{cases} \quad (3)$$



At the receiver end, receiver can easily found  $OP$  and  $NP$  by the key  $\xi$ . For extraction of  $p$  value we use Equation (4).

$$p = \begin{cases} NP - 247, & \text{if } OP > 247 \\ NP - 8, & \text{if } OP < 8 \\ NP - OP, & \text{otherwise.} \end{cases} \quad (4)$$

## 4 Experimental Results and Comparison

Our developed algorithms: data embedding and extraction are implemented in MATLAB Version 7.6.0.324 (R2008a). Here, the impairment is assessed by means of two factors namely, Mean Square Error ( $MSE$ ) and Peak Signal to Noise Ratio ( $PSNR$ ). The  $MSE$  is calculated as by Equation (5)

$$MSE = \frac{\sum_{i=1}^M \sum_{j=1}^N [X(i, j) - Y(i, j)]^2}{(M \times N)}, \quad (5)$$

where  $M$  and  $N$  denote the total number of pixels in the horizontal and the vertical dimensions of the image respectively.  $X(i, j)$  represents the pixels in the cover image and  $Y(i, j)$  represents the pixels of the stego image.

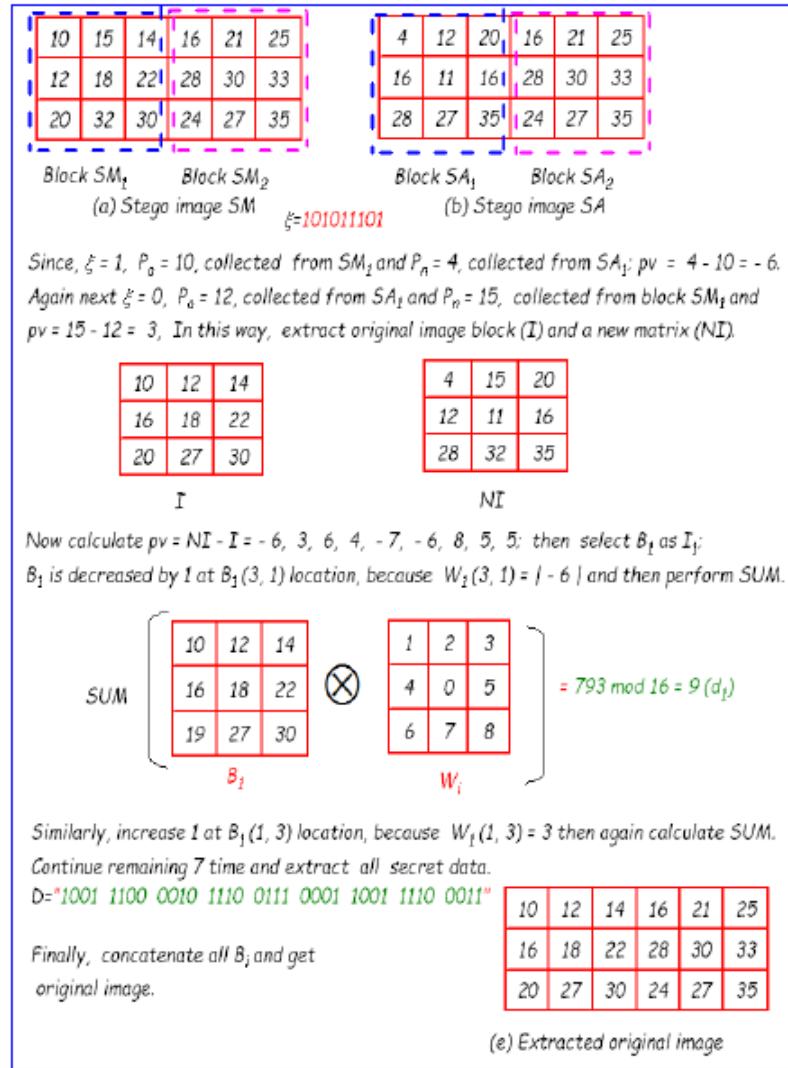


Figure 2: Extraction example

The difference between the original and stego images is assessed by the Peak Signal to Noise Ratio ( $PSNR$ ). The analysis in terms of  $PSNR$  of cover image and stego image shows reasonably good results which is shown in Table 1.

Table 1: Data embedding capacity with PSNR

Image(I)	Data (Bits)	PSNR(SM)	PSNR(SA)
Camera Man	80,000	42.6752	43.1809
	1,60,000	39.7952	40.1716
	2,40,000	37.9778	38.4299
	2,60,096	37.6072	38.0798
House	80,000	42.6101	43.1188
	1,60,000	39.6894	40.1066
	2,40,000	37.9109	38.3755
	2,60,096	37.5586	38.0262
Jet Plane	80,000	42.6988	43.2139
	1,60,000	39.7976	40.1907
	2,40,000	37.9901	38.4492
	2,60,096	37.6146	38.0896
Lake	80,000	42.7090	43.1874
	1,60,000	39.7833	40.1606
	2,40,000	37.9790	38.4355
	2,60,096	37.6212	38.0835
Lena	80,000	42.7090	43.1928
	1,60,000	39.7856	40.1739
	2,40,000	37.9790	38.4502
	2,60,096	37.6379	38.0760
Little Lady	80,000	42.2023	42.6494
	1,60,000	39.5056	39.9096
	2,40,000	37.4163	37.8754
	2,60,096	36.9781	37.4429
Aerial	80,000	42.7000	43.2065
	1,60,000	39.7779	40.1823
	2,40,000	37.9767	38.4491
	2,60,096	37.6206	38.0687
Air Plane	80,000	42.5647	42.9980
	1,60,000	39.6874	40.0926
	2,40,000	37.9419	38.3705
	2,60,096	37.5712	38.0272
boat	80,000	42.6979	43.1925
	1,60,000	39.7214	40.1579
	2,40,000	37.9193	38.4441
	2,60,096	37.5853	38.0103
Clock	80,000	42.6866	43.1936
	1,60,000	39.7922	40.1734
	2,40,000	37.9918	38.4281
	2,60,096	37.6173	38.0780
Moon	80,000	42.6957	43.2003
	1,60,000	39.7922	40.1643
	2,40,000	37.9513	38.4238
	2,60,096	37.5963	38.0592
Baboon	80,000	42.6954	43.2206
	1,60,000	39.7351	40.1254
	2,40,000	37.9923	38.4215
	2,60,096	37.5951	38.0973
Gold-Hill	80,000	42.7115	43.2029
	1,60,000	39.7541	40.1211
	2,40,000	37.9523	38.4255
	2,60,096	37.5901	38.0843
Zelda	80,000	42.6758	43.1753
	1,60,000	39.7202	40.1463
	2,40,000	37.9443	38.4318
	2,60,096	37.5780	38.0073



PSNR is calculated using Equation (6).

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}. \quad (6)$$

Higher the values of PSNR between two images, better the quality of the stego image and very similar to the cover image where as low PSNR demonstrates the opposite. The payload in terms of bits per pixel (bpp) is calculated by the following equation:

$$B = \frac{\frac{m}{x} \times \frac{n}{y} \times ((x \times y) \times r)}{(m \times n \times 2)}, \quad (7)$$

where  $m$  and  $n$  represent size of the input image, that is,  $I_{(m \times n)}$ .  $x$  and  $y$  represent size of the block.  $r$  represents the number of bits which are hidden in each block, 2 represents the number of stego images (dual). Consider  $m = 256$ ,  $n = 256$ ,  $x = 3$ ,  $y = 3$ ,  $r = 4$  and  $s = 2$ . So,  $B = 1.98$  bpp. The standard image are used for experiment. Figure 3 shows the input cover image and Figure 4 shows the dual stego image after embedding 2,60,096 bits.



Figure 3: Inputs images of size (256×256)

Table 2 presents a comparison between the proposed method and existing dual image based data hiding methods. We observed that the average PSNR of the stego images of the proposed method is around 37.7 dB when capacity is 2,60,096. The payload is 1.98 bpp. This capacity is higher than other existing techniques proposed by Lee et al.'s [11], Chang et al.'s [6], Qin et al.'s [21] and Lu et al.'s [16] So, in terms of payload our proposed method is superior, but the PSNR is slightly dropped.

## 5 Steganalysis

Steganalysis is the detection of secret data in stego images. Here, we describe and present the experimental results on J. Fridrich's RS steganalysis [9] and Cachin's KullbackLeibler (KL) divergence [1].

### 5.1 RS Steganalysis

We analyze our stego images by the J. Fridrich's RS steganalysis [9]. When the value of RS analysis is close to zero it means that the scheme is secure. It is observed from Table 3 and Table 4 that the values of  $R_M$  and  $R_{-M}$ ,  $S_M$  and  $S_{-M}$  are nearly equal. Thus rule  $R_M \cong R_{-M}$  and  $S_M \cong S_{-M}$  are satisfied for the stego image in our scheme. So, the proposed method is secure against RS attack.

Table 2: Comparison between dual image based existing methods with our proposed method

Methods	PSNR	Images			
		Lena	Peppers	Boat	Goldhill
Chang et al.	SM	45.12	45.14	45.12	45.13
	SA	45.13	45.15	45.13	45.14
	Avg	45.13	45.15	45.13	45.14
	bpp	1	0.99	1	1
Chang et al.	SM	48.13	48.11	48.13	48.13
	SA	48.14	48.14	48.12	48.15
	Avg	48.14	48.13	48.13	48.14
	bpp	1	1	1	1
Lee et al.	SM	51.14	51.14	51.14	51.14
	SA	54.16	54.17	54.16	54.16
	Avg	52.65	52.66	52.65	52.65
	bpp	0.75	0.75	0.75	0.75
Lee et al.	SM	49.76	49.75	49.76	49.77
	SA	49.56	49.56	49.57	49.57
	Avg	49.66	49.66	49.67	49.67
	bpp	1.07	1.07	1.07	1.07
Chang et al.	SM	39.89	39.94	39.89	39.9
	SA	39.89	39.94	39.89	39.9
	Avg.	39.89	39.94	39.89	39.9
	bpp	1.53	1.52	1.53	1.53
Qin et al.	SM	52.11	51.25	51.11	52.11
	SA	41.34	41.52	41.57	41.34
	Avg.	46.72	46.39	46.84	46.72
	bpp	1.16	1.16	1.16	1.16
Lu et al.	SM	49.20	49.19	49.20	49.23
	SA	49.21	49.21	49.21	49.18
	Avg.	49.21	49.20	49.21	49.21
	bpp	1	0.99	1	1
Our Scheme	SM	37.63	37.61	37.58	37.59
	SA	38.07	38.06	38.01	38.08
	Avg.	37.85	37.83	37.79	37.83
	bpp	<b>1.98</b>	<b>1.98</b>	<b>1.98</b>	<b>1.98</b>

Table 3: RS analysis for Stego images SM of size  $256 \times 256$ )

Image	Data	SM				RS value
		$R_M$	$R_{-M}$	$S_M$	$S_{-M}$	
Cameraman	80000	6896	6922	3807	3817	0.0034
	160000	6403	6451	4270	4237	0.0076
	240000	6074	6138	4496	4468	0.0087
	260096	6152	6122	4527	4479	0.0073
Lena	80000	5490	5586	4142	4050	0.0195
	160000	5427	5550	4280	4149	0.0262
	240000	5422	5586	4424	4312	0.0280
	260096	5484	5535	4406	4448	0.0094
Baboon	80000	5872	5812	5010	5141	0.0176
	160000	5800	5815	5116	5112	0.0017
	240000	5851	5770	5118	5219	0.0166
	260096	5856	5757	5109	5215	0.0187



Figure 4: Stego image of size (256×256)

Table 4: RS analysis for stego images SA of size 256×256)

Image	Data	SA				RS value
		$R_M$	$R_{-M}$	$S_M$	$S_{-M}$	
Cameraman	80000	6961	6954	3788	3770	0.0023
	160000	6537	6422	4190	4248	0.0161
	240000	6179	6278	4426	4405	0.0113
	260096	6278	6244	4420	4447	0.0057
Lena	80000	5572	5483	4071	4100	0.0122
	160000	5476	5570	4308	4214	0.0192
	240000	5475	5452	4299	4354	0.0080
	260096	5409	5602	4495	4338	0.0353
Baboon	80000	5813	5831	5004	5091	0.0097
	160000	5841	5823	5077	5135	0.0070
	240000	5915	5701	5022	5251	0.0405
	260096	5803	5793	5088	5134	0.0051

## 5.2 Kullback-Leibler (K-L) Divergence

K-L divergence is also one of the popular security measures to analyze the data hiding schemes. It has been proposed by Cachin in 1998 [1]. Let  $p_m$  and  $q_n$  be probability measures for original image I and stego image S respectively. The KullbackLeibler (KL) divergence  $D(S||I)$  (also known as Relative Entropy) is defined as Equation (8).

$$D(S||I) = \sum_{x \in G} q_n(x) \log \frac{q_n(x)}{p_m(x)}, \quad (8)$$

where  $x \in G = 0, 1, 2, \dots, 255$  is the pixel value in gray scale images. We design our embedding algorithm such a manner that we get minimum value of K-L divergence which justifies the security. When K-L divergence between two probability distribution functions is zero then the system is perfectly secure.  $D(S||I)$  is a nonnegative continuous function and equals to zero if and only if  $p_m$  and  $q_n$  coincide. Thus  $D(S||I)$  can be naturally viewed as a distance between the measures  $p_m$  and  $q_n$ . In our experiment, it is shown that when the number of characters in the secret message increases, the K-L values in stego image is also increases. The K-L values in our experiment varies between 0.01 to 0.14 which is very less and implies that the proposed scheme provides secure hidden communication. K-L divergence values of cover image are shown in Table 5 and Table 6 shows the K-L values for SM and SA.

Table 5: Relative entropy of original image (256×256)

Cover Image	K-L
Cameraman	7.0299
Lena	7.4429
Baboon	7.2371

Table 6: Relative entropy of stego images SM and SA

Image	Data	SM		SA	
		K-L	Diff.	K-L	Diff.
Cameraman	80000	7.0572	0.04	7.1143	0.02
	160000	7.1220	0.01	7.1143	0.03
	240000	7.1547	0.14	7.1458	0.18
	260096	7.1555	0.14	7.1452	0.12
Lena	80000	7.4491	0.02	7.4494	0.01
	160000	7.4550	0.02	7.4562	0.01
	240000	7.4653	0.03	7.4622	0.03
	260096	7.4668	0.04	7.4654	0.03
Baboon	80000	7.2393	0.04	7.2394	0.04
	160000	7.2438	0.05	7.2437	0.05
	240000	7.2471	0.05	7.2461	0.05
	260096	7.2469	0.05	7.2475	0.05

## 6 Steganographic Attack

We analyze our propose scheme through various stego attacks include statistical attack, Jeremiah J. Harmsena's Histogram attack and brute force attack. We propose our data embedding algorithm which resist against all these types of attacks making eavesdropper unable to retain the hidden message.

### 6.1 Statistical Attack

In this section, we analyze the statistical attacks by finding Standard Deviation ( $SD$ ) and Correlation Coefficient ( $CC$ ) of cover and stego images of our proposed scheme. We calculate the ( $SD$ ) and ( $CC$ ) of cover and stego images that is before and after data embedding which are summarized in Table 7. Minimizing parameters difference is one

of the primary aims in order to get rid of statistical attacks. It is observed that there is no substantial divergence between the  $SD$  of the cover-image and the stego-images. This study shows that the magnitude of change in stego-images based on image parameters is small from a cover image. Since the image parameters have not changed much, the method offers a good concealment of data and reduces the chance of the secret data being detected. Thus, it indicates secure data hiding scheme.

Table 7: Standard deviation (SD) and correlation coefficient (CC) of proposed method

Image	SD			CC		
	I	SM	SA	I & SM	I & SA	SM & SA
Cameraman	61.58	61.70	61.67	0.99	0.99	0.99
Lena	47.83	47.96	47.94	0.99	0.99	0.99
Baboon	38.37	38.48	38.50	0.99	0.99	0.99

## 6.2 Histogram Attack

A new steganalytic attack has been proposed by Jeremiah J. Harmsena [10] in 2003. Harmsen based his attack on the fact that noise adding in the spatial domain corresponds to low-pass filtering of the histogram. Figure 5 describes the histogram of the cover and stego image and their difference histograms. The stego image is produced from cover image employing the maximum data hiding capacity. It is observed that the shape of the histogram is preserved after embedding the secret data. Histogram of cover image is represented as  $h$  whereas histogram of stego image is represented as  $h'$ . The change of histogram can be measured by Equation (9).

$$D_h = \sum_{m=1}^{255} |h'_m - h_m| \quad (9)$$

The difference of the histogram is very small. It is observed that, bins close to zero are more in number and the bins which are away from zero are less in number. This confirms the quality of stego image. There is no step pattern observed which ensures the proposed method is robust against histogram analysis.

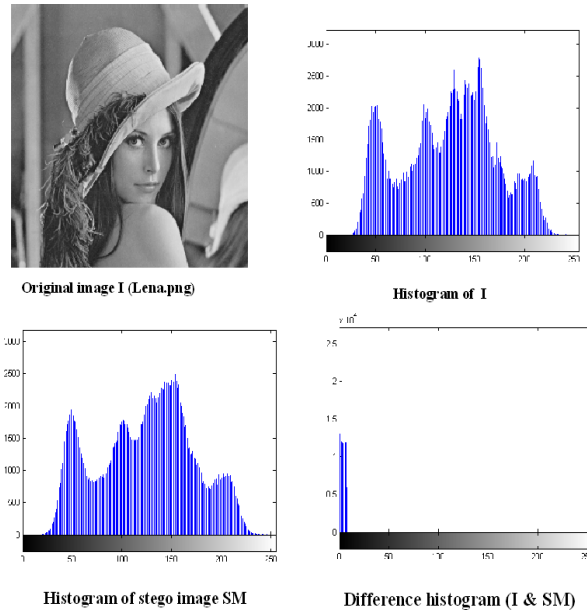


Figure 5: Histogram of original and stego image and their difference

## 6.3 Brute Force Attack

The proposed scheme produces dual stego images which protect secret information through weighted matrix. We embed the data embedding position ( $p$ ), not the original information within dual stego images. We use  $\kappa$  to update

weighted matrix for each selected block. The scheme is secure to prevent possible malicious attacks. Figure 6 shows the example of getting noise data when applied wrong key and wrong weighted matrix are used to reveal the hidden message. If the malicious attacker holds the original image and stego image and is fully aware of the proposed scheme, the hidden message still cannot be correctly revealed without knowing the correct secret key and correct weighted matrix. Similarly, if the malicious attacker are fully aware about stego image and weighted matrix of the proposed scheme, the hidden message still cannot be correctly revealed without knowing the correct key  $\xi$  and  $\kappa$ . Furthermore, the attacker may employ the brute force attack that tries all possible permutation to reveal the hidden message. Maximum possibilities of weighted matrix to embed  $r$  bits data length in each block is  $(2^{r-1} + 1)!$ . We have used  $(M \times N)$  original matrix and partitioned  $(3 \times 3)$  blocks. Total number of blocks are  $\lfloor \frac{M}{3} \rfloor \times \lfloor \frac{N}{3} \rfloor$  and each block is used a modified weighted matrix. So, the number of trials to reveal the hidden message are  $((2^{r-1} + 1)!)^{\lfloor \frac{M}{3} \rfloor \times \lfloor \frac{N}{3} \rfloor}$ . In our scheme, key  $\xi$  is used for pixel distribution among dual image. So, if key length is 128 bits then for  $(256 \times 256)$  image with  $r = 4$ , number of trails will be  $(2^{128} \times 3,62,880)^{7281}$  which is computationally infeasible for current computers by an adversary.

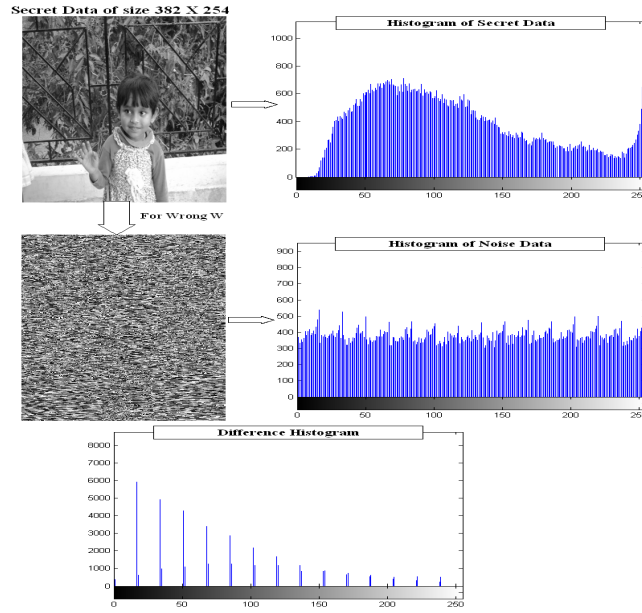


Figure 6: Noise like secret data for wrong weighted matrix

The proposed scheme has achieved stronger robustness against several attacks. Furthermore, the secret information can be retrieved without encountering any loss of data and recovered original image successfully from stego image.

## 7 Conclusion

A new reversible data hiding scheme through weighted matrix using dual image is proposed in this paper. We have modified weighted matrix for different blocks using  $\kappa$  to enhance security in data hiding. In this scheme, we have achieved PSNR greater than 39 dB and payload greater than 1.98 bpp. We have also tested our scheme using RS steganalysis, calculate Kullback-Leibler (K-L) divergence, statistical analysis (such as Standard Deviation and Correlation Coefficient) which have provide promising results. We have tested our scheme by several steganographic attacks such as histogram attack and brute force attack. We have observed that the scheme is secure and robust against all known attacks.

## References

- [1] C. Cachin, "An information-theoretic model for steganography," in *Lecture Notes in Computer Science*, vol. 1525, Springer-Verlag, pp. 306–318, 1998.
- [2] C. Chan, L. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognition*, vol. 37, no. 3, pp. 474–496, 2004.
- [3] C. Chang, C. Chan, Y. Fan, "Image hiding scheme with modulus function and dynamic programming," *Pattern Recognition*, vol. 39, no. 6, pp. 1155–1167, 2006.



- [4] C. Chang, J. Hsiao, C. Chan, "Finding optimal least-significant-bits substitution in image hiding by dynamic programming strategy," *Pattern Recognition*, vol. 36, no. 7, pp. 1583–1595, 2003.
- [5] C. C. Chang, T. D. Kieu, and Y. C. Chou, "Reversible data hiding scheme using two steganographic images," in *Proceedings of IEEE Region 10 International Conference (TENCON'07)*, pp. 1–4, 2007.
- [6] C. C. Chang, T. C. Lu, G. Horng, Y. H. Huang, and Y. M. Hsu, "A high payload data embedding scheme using dual stego-images with reversibility," in *Proceedings of Third International Conference on Information, Communications and Signal Processing*, pp. 1–5, 2013.
- [7] L. Fan, T. Gao, Y. Cao, "Improving the embedding efficiency of weight matrix-based steganography for grayscale images," *Computers and Electrical Engineering*, vol. 39, pp. 873–881, 2013.
- [8] L. Fan, T. Gao, Q. Yang, Y. Cao, "An extended matrix encoding algorithm for steganography of high embedding efficiency," *Computers & Electrical Engineering*, vol. 37, pp. 973–981, 2011.
- [9] J. Fridrich, J. Goljan, R. Du, "Invertible authentication," in *Proceedings of the SPIE, Security and Watermarking of Multimedia Contents*, vol. 4314, San Jose, CA, pp. 197–208, Jan. 2001.
- [10] J. J. Harmsen and W. A. Pearlman, "Steganalysis of additive noise modelable information hiding," in *Proceedings of SPIE Electronic Imaging*, Santa Clara, Jan. 21–24, 2003.
- [11] C. F. Lee and Y. L. Huang, "Reversible data hiding scheme based on dual stego-images using orientation combinations," *Telecommunication Systems*, vol. 52, No. 4, pp. 2237–2247, 2013.
- [12] C. F. Lee, K. H. Wang, C. C. Chang, and Y. L. Huang, "A reversible data hiding scheme based on dual steganographic images," in *Proceedings of the Third International Conference on Ubiquitous Information Management and Communication*, pp. 228–237, 2009.
- [13] P. S. Liao, J. S. Pan, Y. H. Chen, B. Y. Liao, "A lossless watermarking technique for halftone images," in *Proceedings of KES 2005*, LNCS 3682, Springer, pp. 593–599, 2005.
- [14] B. K. Lien, Y. Lin, "High-capacity reversible data hiding by maximum-span pairing," *Multimedia Tools and Applications*, vol. 52, pp. 499–511, 2011.
- [15] C. C. Lin, W. L. Tai, C. C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," *Pattern Recognition*, vol. 41, no. 35, pp. 82–91, 2008.
- [16] T. C. Lu, C. Y. Tseng, and J. H. Wu, "Dual Imaging-based reversible hiding technique using LSB matching," *Signal Processing*, vol. 108, pp. 77–89, 2015.
- [17] Z. M. Lu, H. Luo, J. S. Pan, "Reversible watermarking for error diffused halftone image using statistical features," in *Proceedings of IWDW 2006*, LNCS 4283, Springer, pp. 71–81, 2006.
- [18] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006.
- [19] J. S. Pan, H. Luo, Z. M. Lu, "A lossless watermarking scheme for halftone image authentication," *International Journal of Computer Science and Network Security*, vol. 6, no. 2b, pp. 147–151, 2006.
- [20] F. Peng, X. Li, B. Yang, "Adaptive reversible data hiding scheme based on integer transform," *Signal Process.* vol. 92, pp. 54–62, 2012.
- [21] C. Qin, C. C. Chang, and T. J. Hsu, "Reversible data hiding scheme based on exploiting modification direction with two steganographic images," *Multimedia Tools and Applications*, pp. 1–12, 2014.
- [22] C. Thien, J. Lin, "A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function," *Pattern Recognition*, vol. 36, no. 12, pp. 2875–2881, 2003.
- [23] Y. C. Tseng, Y. Y. Chen, H. K. Pan, "A secure data hiding scheme for binary images," *IEEE Transactions on Communications*, vol. 50, no. 8, pp. 1227–1231, 2002.
- [24] P. Y. Tsai, Y. C. Hu, H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Processing*, vol. 89, no. 11, pp. 29–43, 2009.
- [25] R. Wang, C. Lin, J. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," *Pattern Recognition*, vol. 34, no. 3, pp. 671–683, 2001.
- [26] S. J. Wang, "Steganography of capacity required using modulo operator foreembedding secret image," *Applied Mathematics and Computation*, vol. 164, no. 1, pp. 99–116, 2005.
- [27] A. Westfeld, "F5 - A steganographic algorithm: High capacity despite better steganalysis," *Lect Notes on Computer Science*, vol. 2137, pp. 289–302, 2001.
- [28] F. X. Yu, H. Luo, S. C. Chu, "Lossless data hiding for halftone images," in *Information Hiding and Applications*, Springer, vol. 227, pp. 181–203, 2009.

## Biography

**Biswapati Jana** is currently working as an Assistant Professor in the Department of Computer Science, Vidyasagar University, Paschim Medinipur, India. He received his B. Tech. and M. Tech. degrees in Computer Science and Engineering from University of Calcutta in 1999 and 2002 respectively. He has recently submitted his Ph.D. Thesis

on Design and Implementation of Dual Image based Reversible Data Hiding Techniques. His research interest includes Image Processing, Data Hiding and Steganography. He has published more than 30 papers in National and International Journal and Conferences.



# The Encryption Algorithm AES-RFWKPES32-4

Aripov Mirsaid, Tuychiev Gulom

(Corresponding author: Tuychiev Gulom)

National University of Uzbekistan, Republic of Uzbekistan, Tashkent

Uzbekistan, 700174, Tashkent, VUZ Gorodok

(Email: mirsaidaripov@mail.ru, blasterjon@gmail.com)

(Received Jan. 17, 2016; revised and accepted Mar. 10 & Apr. 9, 2016)

## Abstract

In this paper developed the encryption algorithm AES-RFWKPES32-4 based on network RFWKPES32-4. In encryption algorithm AES-RFWKPES32-4 as a round function selected SubBytes(), ShiftRows(), MixColumns() transformations of encryption algorithm AES. Encryption algorithm consists from four round functions, having four input and output blocks. In encryption algorithm length of block is 1024 bits, the number of rounds is 10, 12, 14 and key length varies from 256 bits to 1024 bits in increments of 128 bits. In the encryption algorithm AES-RFWKPES32-4, like algorithms based on the Feistel network, when encryption and decryption used the same algorithm. It gives convenience of at creating hardware and software-hardware means. With decryption encryption round keys apply in reverse, wherein based operations necessary calculate inversion. Besides, in encryption algorithm applied new S-boxes based design Nyberg and resistance S-boxes equal resistance S-box encryption algorithm AES. Studies show what, encryption speed the encryption algorithms AES-RFWKPES32-4 faster than AES

*Keywords: Advanced Encryption Standard; Feistel Network; Lai-Massey Scheme; Output Transformation; Round Function; Round Keys*

## 1 Introduction

In September 1997, the National Institute of Standards and Technology issued a public call for proposals for a new block cipher to succeed the Data Encryption Standard [28]. Out of 15 submitted algorithms the Rijndael cipher by Daemen and Rijmen [3] was chosen to become the new Advanced Encryption Standard in November 2001 [4]. The Advanced Encryption Standard is a block cipher with a fixed block length of 128 bits. It supports three different key lengths: 128 bits, 192 bits, and 256 bits. Encrypting a 128-bit block means transforming it in  $n$  rounds into a 128-bit output block. The number of rounds  $n$  depends on the key length:  $n=10$  for 128-bit keys,  $n=12$  for 192-bit keys, and  $n=14$  for 256-bit keys. The 16-byte input block  $(t_0, t_1, \dots, t_{15})$  which is transformed during encryption is usually written as a 4x4 byte matrix, the called AES *State*.

$t_0$	$t_4$	$t_8$	$t_{12}$
$t_1$	$t_5$	$t_9$	$t_{13}$
$t_2$	$t_6$	$t_{10}$	$t_{14}$
$t_3$	$t_7$	$t_{11}$	$t_{15}$

The structure of each round of AES can be reduced to four basic transformations occurring to the elements of the *State*. Each round consists in applying successively to the *State* the SubBytes(), ShiftRows(), MixColumns() and AddRoundKey() transformations. The first round does the same with an extra AddRoundKey() at the beginning whereas the last round excludes the MixColumns() transformation.

The SubBytes() transformation is a nonlinear byte substitution that operates independently on each byte of the *State* using a substitution table (S-box). Figure 1 illustrates the SubBytes() transformation on the *State*.

In the ShiftRows() transformation operates on the rows of the *State*; it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left.

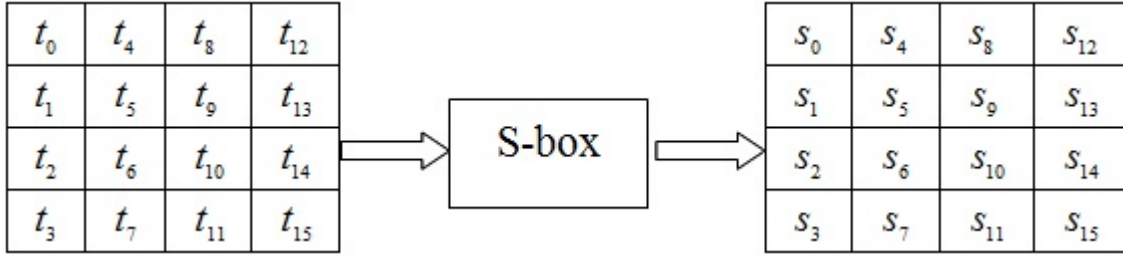


Figure 1: SubBytes() transformation

Similarly, the third and fourth rows are shifted by offsets of two and three respectively. Figure 2 illustrates the ShiftRows() transformation.

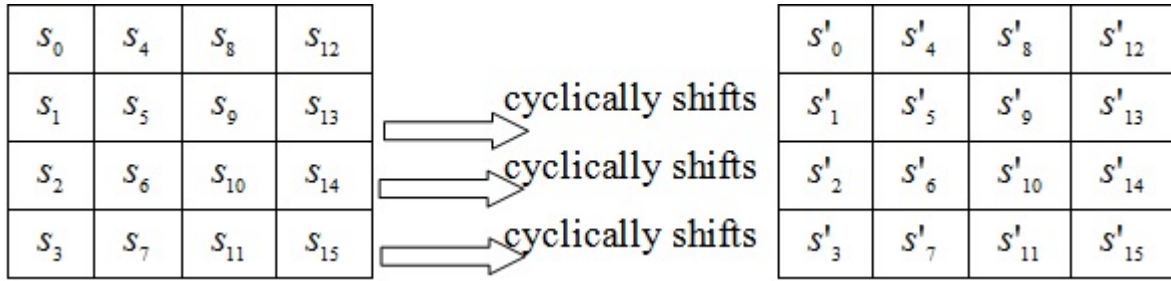


Figure 2: ShiftRows() transformation

The MixColumns() transformation operates on the *State* column-by-column, treating each column as a four-term polynomial. The columns are considered as polynomials over  $GF(2^8)$  and multiplied modulo  $x^4 + 1$  with a fixed polynomial  $a(x)$ , given by  $a(x) = 3x^2 + x^2 + x + 2$ . Let  $p = a(x) \otimes s'$ :

$$\begin{bmatrix} p_{4i} \\ p_{4i+1} \\ p_{4i+2} \\ p_{4i+3} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s'_{4i} \\ s'_{4i+1} \\ s'_{4i+2} \\ s'_{4i+3} \end{bmatrix}, \quad i = \overline{0 \dots 3}$$

As a result of this multiplication, the four bytes in a column are replaced by the following:

$$\begin{aligned} y_{4i} &= (\{02\} \bullet s'_{4i}) \oplus (\{03\} \bullet s'_{4i+1}) \oplus s'_{4i+2} \oplus s'_{4i+3} \\ y_{4i+1} &= s'_{4i} \oplus (\{02\} \bullet s'_{4i+1}) \oplus (\{03\} \bullet s'_{4i+2}) \oplus s'_{4i+3} \\ y_{4i+2} &= s'_{4i} \oplus s'_{4i+1} \oplus (\{02\} \bullet s'_{4i+2}) \oplus (\{03\} \bullet s'_{4i+3}) \\ y_{4i+3} &= (\{03\} \bullet s'_{4i}) \oplus s'_{4i+1} \oplus s'_{4i+2} \oplus (\{02\} \bullet s'_{4i+3}). \end{aligned}$$

Figure 3 illustrates the MixColumns() transformation.

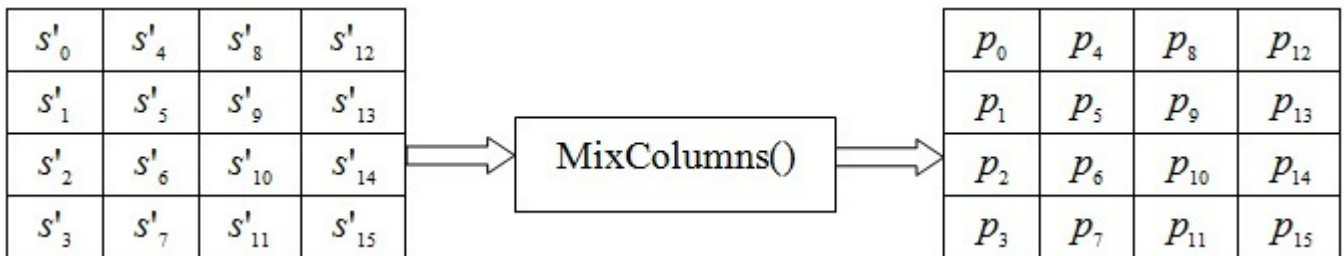


Figure 3: MixColumns() transformation

On the basis of encryption algorithm PES and scheme Lai-Massey developed the networks PES32-4 and RFWKPES32-4, consisting from one round function [6, 17]. In the networks PES32-4 and RFWKPES32-4, similarly as in the Feistel network, when encryption and decryption using the same algorithm. In the networks used four round function having four input and output blocks and as the round function can use any transformation.

Using transformation SubBytes(), ShiftRows(), MixColumns(), AddRoundKey() AES encryption algorithm as a round function networks IDEA8-1, RFWKIDEA8-1 [7], PES8-1 [9], RFWKPES8-1 [12], IDEA16-1 [5], RFWKIDEA16-1 [10], PES16-1 [15], RFWKPES16-1 [16], RFWKIDEA32-1 [17], PES32-1 [8], RFWKPES32-1 [11], IDEA16-2 [5], RFWKIDEA16-2 [10], IDEA32-4 [6], RFWKIDEA32-4 [17], PES16-2 [15], RFWKPES16-2 [16], created encryption algorithms AES-IDEA8-1 [25], AES-RFWKIDEA8-1 [27], AES-PES8-1 [26], AES-RFWKPES8-1 [14], AES-IDEA16-1 [24], AES-RFWKIDEA16-1 [20], AES-PES16-1, AES-RFWKPES16-1 [22], AES-RFWKIDEA32-1 [21], AES-PES32-1, AES-RFWKPES32-1 [18], AES-IDEA16-2, AES-RFWKIDEA16-2 [2], AES-IDEA32-4, AES-RFWKIDEA32-4 [19], AES-PES16-2, AES-RFWKPES16-2 [23].

In this paper developed block encryption algorithm AES-RFWKPES32-4 based network RFWKPES32-4 [11] using transformation of the encryption algorithm AES. The length of block of the encryption algorithms is 1024 bits, the number of rounds  $n$  equal to 10, 12, 14 and the length of key is variable from 256 bits to 1024 bits in steps 128 bits, i.e., key length is equal to 256, 384, 512, 640, 768, 896 and 1024 bits.

## 2 The Encryption Algorithm AES-RFWKPES32-4

### 2.1 The Structure of the Encryption Algorithm AES-RFWKPES32-4

In the encryption algorithm AES-RFWKPES32-4 as the round function used SubBytes(), ShiftRows(), MixColumns() transformation encryption algorithm AES. The scheme  $n$ -rounded encryption algorithm AES-RFWKPES32-4 is presented in Figure 4, and the length of subblocks  $X^0, X^1, \dots, X^{31}$ , length of round keys  $K_{32(i-1)}, K_{32(i-1)+1}, \dots, K_{32(i-1)+31}, i = \overline{1 \dots n+1}$  and  $K_{32n+32}, K_{32n+33}, \dots, K_{32n+95}$  are 32-bits.

Consider the round function of the encryption algorithm AES-RFWKPES32-4. Initially 32-bit subblocks  $T^0, T^1, \dots, T^{15}$  into split to 8-bit subblocks  $t_0^0, t_1^0, \dots, t_{15}^0, t_0^1, t_1^1, \dots, t_{15}^1, t_0^2, t_1^2, \dots, t_{15}^2, t_0^3, t_1^3, \dots, t_{15}^3$  as follows:

$$\begin{aligned} t_i^0 &= sb_{imod4}(T^{div4}), \\ t_i^1 &= sb_{imod4}(T^{div4+4}), \\ t_i^2 &= sb_{imod4}(T^{div4+8}), \\ t_i^3 &= sb_{imod4}(T^{div4+12}), i = \overline{0, 1, \dots, 15}, \end{aligned}$$

where div-the integer part of division, mod-remainder of the division,

$$\begin{aligned} sb_0(X) &= x_0x_1\dots x_7, \\ sb_1(X) &= x_8x_9\dots x_{15}, \\ sb_2(X) &= x_{16}x_{17}\dots x_{23}, \\ sb_3(X) &= x_{24}x_{25}\dots x_{31} \end{aligned}$$

and

$$\begin{aligned} T^0 &= t_0^0 || t_1^0 || t_2^0 || t_3^0, \\ T^1 &= t_4^0 || t_5^0 || t_6^0 || t_7^0, \\ T^2 &= t_8^0 || t_9^0 || t_{10}^0 || t_{11}^0, \\ T^3 &= t_{12}^0 || t_{13}^0 || t_{14}^0 || t_{15}^0, \\ T^4 &= t_0^1 || t_1^1 || t_2^1 || t_3^1, \\ T^5 &= t_4^1 || t_5^1 || t_6^1 || t_7^1, \\ T^6 &= t_8^1 || t_9^1 || t_{10}^1 || t_{11}^1, \\ T^7 &= t_{12}^1 || t_{13}^1 || t_{14}^1 || t_{15}^1, \\ T^8 &= t_0^2 || t_1^2 || t_2^2 || t_3^2, \\ T^9 &= t_4^2 || t_5^2 || t_6^2 || t_7^2, \\ T^{10} &= t_8^2 || t_9^2 || t_{10}^2 || t_{11}^2, \\ T^{11} &= t_{12}^2 || t_{13}^2 || t_{14}^2 || t_{15}^2, \end{aligned}$$

$$\begin{aligned}
T^{12} &= t_0^3 || t_1^3 || t_2^3 || t_3^3, \\
T^{13} &= t_4^3 || t_5^3 || t_6^3 || t_7^3, \\
T^{14} &= t_8^3 || t_9^3 || t_{10}^3 || t_{11}^3, \\
T^{15} &= t_{12}^3 || t_{13}^3 || t_{14}^3 || t_{15}^3.
\end{aligned}$$

As elements of State array of the first round functions are chosen subblocks  $t_0^0, t_1^0, \dots, t_{15}^0$ , second round function are chosen subblocks  $t_0^1, t_1^1, \dots, t_{15}^1$ , third round function are chosen subblocks  $t_0^2, t_1^2, \dots, t_{15}^2$  and fourth round function are chosen subblocks  $t_0^3, t_1^3, \dots, t_{15}^3$ .

The 8-bit subblocks  $t_0^0, t_1^0, \dots, t_{15}^0$  are written into the  $State_0$  array, subblocks  $t_0^1, t_1^1, \dots, t_{15}^1$  are written into the  $State_1$  array, subblocks  $t_0^2, t_1^2, \dots, t_{15}^2$  are written into the  $State_2$  array, subblocks  $t_0^3, t_1^3, \dots, t_{15}^3$  are written into the  $State_3$  array and are executed the SubBytes(), ShiftRows(), MixColumns() transformations. After the MixColumns() transformation 8-bit output values combined and is obtained 32-bit subblocks  $Y^0, Y^1, \dots, Y^{15}$ .

Here  $Y^0, Y^1, Y^2, Y^3$  - output subblocks first round function,  $Y^4, Y^5, Y^6, Y^7$  - output subblocks second round function,  $Y^8, Y^9, Y^{10}, Y^{11}$  - output subblocks third round function,  $Y^{12}, Y^{13}, Y^{14}, Y^{15}$  - output subblocks fourth round function and

$$\begin{aligned}
Y^0 &= p_0^0 || p_1^0 || p_2^0 || p_3^0, \\
Y^1 &= p_4^0 || p_5^0 || p_6^0 || p_7^0, \\
Y^2 &= p_8^0 || p_9^0 || p_{10}^0 || p_{11}^0, \\
Y^3 &= p_{12}^0 || p_{13}^0 || p_{14}^0 || p_{15}^0, \\
Y^4 &= p_0^1 || p_1^1 || p_2^1 || p_3^1, \\
Y^5 &= p_4^1 || p_5^1 || p_6^1 || p_7^1, \\
Y^6 &= p_8^1 || p_9^1 || p_{10}^1 || p_{11}^1, \\
Y^7 &= p_{12}^1 || p_{13}^1 || p_{14}^1 || p_{15}^1, \\
Y^8 &= p_0^2 || p_1^2 || p_2^2 || p_3^2, \\
Y^9 &= p_4^2 || p_5^2 || p_6^2 || p_7^2, \\
Y^{10} &= p_8^2 || p_9^2 || p_{10}^2 || p_{11}^2, \\
Y^{11} &= p_{12}^2 || p_{13}^2 || p_{14}^2 || p_{15}^2, \\
Y^{12} &= p_0^3 || p_1^3 || p_2^3 || p_3^3, \\
Y^{13} &= p_4^3 || p_5^3 || p_6^3 || p_7^3, \\
Y^{14} &= p_8^3 || p_9^3 || p_{10}^3 || p_{11}^3, \\
Y^{15} &= p_{12}^3 || p_{13}^3 || p_{14}^3 || p_{15}^3.
\end{aligned}$$

The S-box SubBytes() transformation shown in Tables 1-4 and is the only nonlinear transformation. The length of the input and output blocks S-box is eight bits. First S-box applied on first round functions, second S-box applied on second round functions, third S-box applied on third round functions and fourth S-box applied on fourth round functions.

Consider the encryption process of encryption algorithm AES-RFWKPES32-4. Initially the 1024-bit plaintext  $X$  partitioned into subblocks of 32-bits  $X_0^0, X_0^1, \dots, X_0^{31}$ , and performs the following steps:

- 1) subblocks  $X_0^0, X_0^1, \dots, X_0^{31}$  summed by XOR respectively with round key  $K_{32n+32}, K_{32n+33}, \dots, K_{32n+63}$ :  
 $X_0^j = X_0^j \oplus K_{32n+32+j}, j = \overline{0...31}$ .
- 2) subblocks  $X_0^0, X_0^1, \dots, X_0^{31}$  multiplied and summed respectively with the round keys  $K_{32(i-1)}, K_{32(i-1)+1}, \dots, K_{32(i-1)+31}$  and calculated 32-bit subblocks  $T^0, T^1, \dots, T^{15}$ . This step can be represented as follows:  
 $T^j = (X_{i-1}^j + K_{32(i-1)+j}) \oplus (X_{i-1}^{j+16} \cdot K_{32(i-1)+16+j}), j = \overline{0...15}, i = 1$ .
- 3) subblocks  $T^0, T^1, \dots, T^{15}$  recorded in four arrays State and performed SubBytes(), ShiftRows(), MixColumns() transformation. Output subblocks of the round functions are  $Y^0, Y^1, \dots, Y^{15}$ .
- 4) subblocks  $Y^0, Y^1, \dots, Y^{15}$  are summed to XOR with subblocks  $X_{i-1}^0, X_{i-1}^1, \dots, X_{i-1}^{31}$ , i.e.  $X_{i-1}^j = X_{i-1}^j \oplus Y^{15-j}$ ,  
 $X_{i-1}^{j+16} = X_{i-1}^{j+16} \oplus Y^{15-j}, j = \overline{0...15}, i = 1$ .
- 5) at the end of the round all subblocks swapped, i.e.,  $X_i^j = X_{i-1}^{16+j}, X_i^{j+16} = X_{i-1}^j, j = \overline{0...15}, i = 1$ .
- 6) repeating steps 2-5  $n$  times, i.e.,  $i = \overline{2...n}$  obtain subblocks  $X_n^0, X_n^1, \dots, X_n^{31}$ .



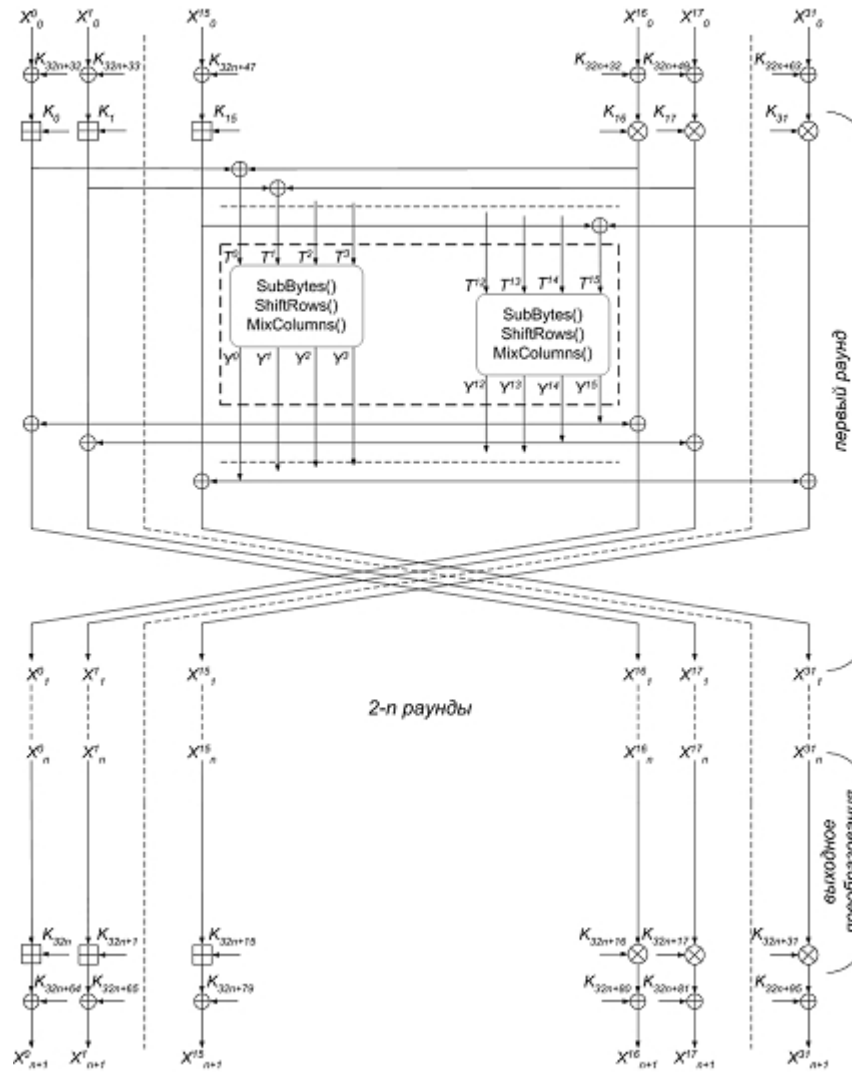


Figure 4: The scheme  $n$ -rounded encryption algorithm AES-RFWKPES32-1

Table 1: First S-box of encryption algorithm AES-RFWKPES32-4

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0x0	0xFE	0x90	0x1B	0xA1	0x0C	0x97	0x44	0x12	0x26	0x49	0x2D	0x9B	0xB6	0x86	0x1F	0x5B
0x1	0x4A	0x2F	0xA8	0xD0	0x65	0x1A	0x34	0xAE	0x6E	0x64	0x36	0xCC	0x01	0x47	0x88	0x81
0x2	0x93	0x54	0x59	0x61	0x57	0x7E	0x9F	0x3B	0xF5	0x07	0x0B	0xEE	0x6A	0xDE	0x66	0xAC
0x3	0xDA	0xB0	0xF2	0x63	0x56	0xCA	0x9A	0x70	0x38	0x9D	0x8D	0x3A	0x13	0x21	0x00	0xB9
0x4	0x20	0x6F	0xAA	0xF4	0xB4	0x04	0xF8	0x94	0x91	0xAD	0xC6	0x40	0x39	0x7A	0x48	0x5E
0x5	0xD1	0xF7	0x09	0x62	0x10	0x14	0xE2	0xB8	0xD7	0x0A	0xBA	0x0F	0xCE	0xBF	0x5A	0xD9
0x6	0xB7	0xC0	0x5F	0x25	0xE7	0xFF	0xC4	0x1E	0x96	0x87	0xAB	0x72	0x33	0x9C	0xE3	0xFD
0x7	0x73	0x76	0x05	0xD5	0x19	0x41	0x4F	0x3D	0x18	0xD3	0x7C	0x50	0x3F	0xF6	0x4C	0x15
0x8	0x7B	0xB3	0xDD	0x22	0x6B	0x8A	0xD6	0x0E	0x52	0xA5	0x32	0xDC	0xCF	0xC9	0x16	0xC8
0x9	0x1C	0xCD	0x5D	0x0D	0xB2	0xDB	0xBB	0xE4	0x74	0x80	0xCB	0xEC	0xAF	0x2B	0x82	0x3C
0xA	0x98	0x84	0xED	0xC2	0x2C	0x78	0xC3	0x89	0x23	0x55	0x2E	0xBE	0xFB	0x28	0x4B	0x03
0xB	0xA9	0xE8	0x17	0xE6	0x77	0x24	0x1D	0xBD	0xA6	0x42	0x7D	0x53	0x8F	0xE1	0x8C	0x60
0xC	0x69	0x43	0x83	0x08	0x85	0xE5	0x71	0xF0	0xF1	0x4D	0xF9	0x67	0x8E	0x58	0x06	0x46
0xD	0x2A	0x3E	0x31	0x6D	0x6C	0xEB	0xDF	0x11	0x5C	0xB5	0x02	0x8B	0xFC	0xC1	0xC5	0xA3
0xE	0xD8	0xC7	0xD2	0x7F	0x35	0x9E	0x95	0x68	0x30	0x27	0xBC	0xB1	0x99	0xA0	0x79	0xEF
0xF	0x37	0xD4	0xA4	0xF3	0xFA	0xE9	0xA7	0x75	0x45	0x92	0xEA	0x51	0xA2	0xE0	0x29	0x4E



Table 2: Second S-box of encryption algorithm AES-RFWKPES32-4

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0x0	0x07	0xDE	0x20	0x1A	0xDD	0x11	0x3D	0x97	0x26	0x18	0x2B	0xD3	0xE7	0xC4	0xB2	0x90
0x1	0x45	0x91	0xAD	0x6E	0xCB	0xC7	0xAE	0x85	0xC6	0x2C	0x14	0x9E	0xF8	0x60	0xBC	0x0B
0x2	0x83	0x0F	0x2A	0x59	0x52	0xF4	0x41	0x31	0x0A	0xD0	0x12	0x35	0x54	0x16	0x96	0x3F
0x3	0x84	0xCF	0xC5	0xE3	0xB5	0xB6	0x34	0x8C	0x6C	0xFB	0xC9	0xD6	0x70	0xE9	0x1F	0x78
0x4	0x0E	0x21	0x17	0xED	0x5D	0x8D	0x2F	0x4C	0x39	0xD8	0x74	0xAF	0x8B	0x66	0xFF	0xE5
0x5	0x89	0xB0	0xA8	0x04	0x2D	0xBF	0xF7	0x9F	0xA1	0xF5	0x25	0x80	0x24	0x50	0x77	0xD9
0x6	0x00	0x5C	0x02	0x7B	0x82	0xE0	0xCE	0x55	0xF6	0x23	0xF0	0x36	0x61	0x1C	0x10	0x5A
0x7	0xD1	0xA4	0x6A	0x1B	0x9A	0x48	0x30	0x19	0x7D	0x33	0x4E	0x9D	0xA3	0x57	0x6D	0x58
0x8	0x81	0x92	0x4B	0xB4	0xB3	0x06	0x46	0x67	0x27	0x88	0x86	0xAC	0xC3	0xEB	0x05	0x0C
0x9	0xEF	0x79	0xB8	0x3A	0x75	0x63	0xC2	0xDF	0x1E	0xEC	0x51	0x8F	0x62	0x03	0x56	0xFE
0xA	0x8E	0x7E	0x68	0xE6	0xCC	0xDC	0x01	0x5B	0x53	0xE8	0x76	0xB7	0x72	0x5E	0xA2	0x42
0xB	0x4A	0x1D	0xE2	0x65	0x43	0x9C	0x08	0xEA	0xD5	0x15	0xA9	0xC0	0x73	0xAA	0x2E	0xBE
0xC	0x09	0xF2	0xB1	0x4F	0x99	0x38	0x6B	0x7F	0x98	0x8A	0xC8	0x71	0x94	0xCD	0x37	0x87
0xD	0xE4	0x44	0xDB	0x9B	0x7C	0x40	0xF1	0xCA	0x5F	0xBA	0xA5	0xE1	0xBD	0xBB	0x29	0xA0
0xE	0x3E	0x93	0xD4	0x13	0x49	0xA6	0xAB	0xEE	0x3C	0xC1	0x0D	0x28	0x69	0xFD	0x3B	0xD2
0xF	0xF3	0xFC	0x6F	0x22	0x95	0xFA	0x32	0xF9	0xDA	0x64	0xA7	0x7A	0x47	0x4D	0xB9	0xD7

Table 3: Third S-box of encryption algorithm AES-RFWKPES32-4

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0x0	0xE0	0x86	0x57	0x8E	0xB1	0x94	0x39	0xAC	0x78	0x97	0x4D	0xB3	0x68	0xE9	0x02	0xAD
0x1	0xD0	0x83	0x75	0x7C	0xC5	0xDE	0x42	0xEE	0xF0	0x4C	0x8C	0xAF	0x1F	0x7E	0x00	0xFB
0x2	0xC1	0xCD	0x63	0x90	0x8A	0x04	0xE6	0x22	0xD5	0x84	0xA3	0x14	0xA5	0x95	0x82	0x20
0x3	0xC0	0xF3	0xC7	0x5E	0x03	0x34	0x3A	0xED	0x65	0x28	0xDC	0xAB	0x25	0x6A	0x96	0x08
0x4	0xE3	0x79	0xBB	0x5C	0xA6	0xC3	0x7B	0xD3	0x0F	0xA9	0x13	0x6C	0xEC	0x51	0x1E	0x71
0x5	0xF5	0x1B	0x6D	0xD7	0x62	0x37	0x33	0x81	0x6E	0x2A	0x4F	0xF6	0x61	0x93	0x24	0x87
0x6	0xE1	0x88	0xF8	0x3F	0xEF	0x69	0xDD	0x8B	0x1D	0x60	0x32	0x23	0x50	0xA1	0xBA	0xA7
0x7	0xAA	0x76	0x4A	0xA0	0x99	0xE5	0x0C	0xB9	0x10	0x3B	0xCA	0x98	0x77	0x92	0x4B	0xBE
0x8	0xD8	0xB4	0xD2	0x2D	0x2C	0xCE	0xE7	0x7F	0x56	0xDB	0xD9	0x5B	0xE8	0x73	0xF9	0xFA
0x9	0x45	0x26	0x36	0x38	0x3D	0x49	0xC6	0xA8	0xB8	0x72	0xBD	0xDA	0x67	0xD6	0xBC	0x30
0xA	0xF4	0x27	0x53	0x46	0xC4	0x9F	0xCF	0x89	0xA4	0x44	0x0A	0x1A	0x3C	0x91	0x59	0xD1
0xB	0xFC	0x8F	0x70	0x66	0xFF	0xB6	0xCC	0x5D	0x9C	0xA2	0x43	0xDF	0x12	0x74	0x55	0x19
0xC	0xE2	0x2B	0x35	0xE4	0xAE	0x21	0x64	0x09	0x80	0xC2	0xF2	0x0B	0x9B	0xEA	0x0D	0xF7
0xD	0x5F	0xFE	0x9E	0xB7	0x3E	0xC8	0x1C	0xEB	0xBF	0x2F	0x58	0x47	0x2E	0x01	0x54	0x40
0xE	0x0E	0x9A	0xB2	0x8D	0xCB	0x6F	0x5A	0x6B	0x17	0xF1	0xD4	0x7A	0x7D	0x07	0x16	0x9D
0xF	0x05	0x29	0x52	0x4E	0xB5	0x06	0x15	0x31	0xB0	0x48	0x41	0x11	0xC9	0xFD	0x18	0x85



Table 4: Fourth S-box of encryption algorithm AES-RFWKPES32-4

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0x0	0x7F	0xE1	0xA8	0xCD	0x3A	0xA3	0x1A	0x4F	0x1F	0xA0	0xC6	0x38	0x5F	0x52	0xF5	0x4E
0x1	0xBF	0xF8	0x2A	0x07	0xE6	0x89	0xF1	0x49	0x3F	0xC7	0xCF	0x4C	0x80	0x05	0xF7	0x10
0x2	0xFE	0xCA	0x70	0xBB	0xD5	0xEF	0x65	0x75	0xA6	0xE3	0x78	0xAF	0x62	0xA2	0xF9	0x77
0x3	0xFF	0x3C	0xE4	0x85	0xF4	0x2F	0x19	0x4A	0x6A	0x5B	0x8B	0x54	0x6E	0x5D	0xA1	0xDB
0x4	0x7C	0x1E	0x14	0x87	0x61	0xFC	0x1C	0xBC	0xC0	0x56	0xB4	0x47	0x4B	0xB2	0x81	0x32
0x5	0x26	0x98	0x46	0xA4	0x71	0x2C	0x34	0xFA	0x45	0x59	0xC4	0x25	0x72	0xB8	0x6F	0xE0
0x6	0x7E	0xD7	0x13	0x00	0x48	0x5E	0x8A	0xD4	0x82	0x73	0x35	0x74	0xB3	0x7A	0x15	0x60
0x7	0x55	0x29	0xDD	0x7B	0x96	0x66	0xC3	0x16	0xB7	0x18	0xD1	0x97	0x28	0xB9	0xDC	0x0D
0x8	0x93	0x23	0xBD	0x42	0x43	0xC9	0x64	0x04	0xA9	0x90	0x92	0x9C	0x53	0x30	0x12	0x11
0x9	0xEA	0x6D	0x2D	0x1B	0x02	0xDE	0xE5	0x57	0x17	0x31	0x0E	0x91	0x68	0xA5	0x0F	0x37
0xA	0x27	0x6C	0xB0	0xE9	0xE7	0x8C	0xC8	0xD6	0x63	0xEB	0xD9	0x99	0x03	0xBA	0x9E	0xBE
0xB	0x0B	0xCC	0x33	0x69	0x08	0x21	0xCB	0x86	0x8F	0x79	0xF0	0x88	0xB5	0x2B	0xAA	0x9A
0xC	0x7D	0x58	0x2E	0x67	0x4D	0x76	0x6B	0xDA	0xFB	0xFD	0x3D	0xD8	0x94	0x51	0xC2	0x24
0xD	0x84	0x09	0x8D	0x20	0x01	0xD3	0x83	0x50	0x0C	0x40	0x9F	0xE8	0x41	0xF6	0xAB	0xF3
0xE	0xC1	0x95	0x39	0xCE	0xD0	0x44	0x9D	0x5C	0xAC	0x3E	0xA7	0x1D	0x06	0xEC	0xAD	0x8E
0xF	0xEE	0x5A	0xB1	0xC5	0x22	0xED	0xAE	0x36	0x3B	0xDF	0xF2	0xB6	0xD2	0x0A	0x9B	0xE2

7) in output transformation round keys  $K_{32n}, K_{32n+1}, \dots, K_{32n+31}$  are multiplied and summed into subblocks, i.e.  $X_{n+1}^j = X_n^j + K_{32n+j}, X_{n+1}^{j+16} = X_n^{j+16} \cdot K_{32n+16+j}, j = 0 \dots 15$ .

8) subblocks  $X_{n+1}^0, X_{n+1}^1, \dots, X_{n+1}^{31}$  are summed to XOR with the round key  $K_{32n+64}, K_{32n+65}, \dots, K_{32n+95}$ :  $X_{n+1}^j = X_{n+1}^j \oplus K_{32n+64+j}, j = 0 \dots 31$ .

As ciphertext plaintext  $X$  accepted the combined 32-bit subblocks  $X_{n+1}^0 || X_{n+1}^1 || \dots || X_{n+1}^{31}$ .

## 2.2 Key Generation of the Encryption Algorithm AES-RFWKPES32-4

In  $n$ -round encryption algorithm AES-RFWKPES32-4 in each round we applied thirty two round keys of the 32-bit and output transformation thirty two round keys of the 32-bit. In addition, before the first round and after the output transformation we used thirty two round keys of 32-bits. Total number of 32-bit round keys is equal to  $32n+96$ . In Figure 4 encryption used encryption round keys  $K_i^c$  instead of  $K_i$ , while decryption used decryption round keys  $K_i^d$ . If  $n=10$  then need 416 to generate round keys, if  $n=12$ , you need to generate 480 round keys and if  $n=14$  need 544 to generate round keys.

When generating round keys like the AES encryption algorithm uses an array Rcon: Rcon=[0x00000001, 0x00000002, 0x00000004, 0x00000008, 0x00000010, 0x00000020, 0x00000040, 0x00000080, 0x00000100, 0x00000200, 0x00000400, 0x00000800, 0x00001000, 0x00002000, 0x00004000, 0x00008000, 0x00010000, 0x00020000, 0x00040000, 0x00080000, 0x00100000, 0x00200000, 0x00400000, 0x00800000, 0x01000000, 0x02000000, 0x04000000, 0x08000000, 0x10000000, 0x20000000, 0x40000000, 0x80000000].

The key encryption algorithm  $K$  of length  $l$  ( $256 \leq l \leq 1024$ ) bits is divided into 32-bit round keys  $K_0^c, K_1^c, \dots, K_{Lenght-1}^c$ ,  $Lenght = l/32$ , here  $K = \{k_0, k_1, \dots, k_{l-1}\}$ ,  $K_0^c = \{k_0, k_1, \dots, k_{31}\}$ ,  $K_1^c = \{k_{32}, k_{33}, \dots, k_{63}\}, \dots, K_{Lenght-1}^c = \{k_{l-32}, k_{l-31}, \dots, k_{l-1}\}$  and  $K = K_0^c || K_1^c || \dots || K_{Lenght-1}^c$ .

Then we calculate  $K_L = K_0^c \oplus K_1^c \oplus \dots \oplus K_{Lenght-1}^c$ . If  $K_L = 0$  then  $K_L$  is chosen as 0xC5, i.e.  $K_L = 0xC5$ . When generating a round keys  $K_i^c, i = Lenght \dots 32n + 95$ , used transformation  $SubBytes32()$  and  $RotWord32()$ , here  $SubBytes32()$ -is transformation 32-bit subblock into S-box,  $SubBytes32(X) = S_0(sb_0(X)) || S_1(sb_1(X)) || S_2(sb_2(X)) || S_3(sb_3(X))$ ,  $S_0$ -first S-box,  $S_1$ -second S-box,  $S_2$ -third S-box,  $S_3$ -fourth S-box and  $RotWord32()$ -cyclic shift to the left of 1 bit of the 32-bit subblock. When the condition  $i \bmod 3 = 1$  is true, then the round keys are computed as  $K_i^c = SubBytes32(K_{i-Lenght+1}^c) \oplus SubBytes32(RotWord32(K_{i-Lenght}^c)) \oplus Rcon[i \bmod 32] \oplus K_L$ , otherwise  $K_i^c = SubBytes32(K_{i-Lenght}^c) \oplus SubBytes(K_{i-Lenght+1}^c) \oplus K_L$ . After each round key generation the value  $K_L$  is cyclic shift to the left by 1 bit.

Decryption round keys are computed on the basis of encryption round keys and decryption round keys of the

output transformation associate with of encryption round keys as follows:

$$\begin{aligned}
 & (K_{32n}^d, K_{32n+1}^d, K_{32n+2}^d, K_{32n+3}^d, K_{32n+4}^d, K_{32n+5}^d, K_{32n+6}^d, K_{32n+7}^d, K_{32n+8}^d, \\
 & K_{32n+9}^d, K_{32n+10}^d, K_{32n+11}^d, K_{32n+12}^d, K_{32n+13}^d, K_{32n+14}^d, K_{32n+15}^d, K_{32n+16}^d, \\
 & K_{32n+17}^d, K_{32n+18}^d, K_{32n+19}^d, K_{32n+20}^d, K_{32n+21}^d, K_{32n+22}^d, K_{32n+23}^d, K_{32n+24}^d, \\
 & K_{32n+25}^d, K_{32n+26}^d, K_{32n+27}^d, K_{32n+28}^d, K_{32n+29}^d, K_{32n+30}^d, K_{32n+31}^d) \\
 = & (-K_0^c, -K_1^c, -K_2^c, -K_3^c, -K_4^c, -K_5^c, -K_6^c, -K_7^c, -K_8^c, \\
 & -K_9^c, -K_{10}^c, -K_{11}^c, -K_{12}^c, -K_{13}^c, -K_{14}^c, -K_{15}^c, (K_{16}^c)^{-1}, \\
 & (K_{17}^c)^{-1}, (K_{18}^c)^{-1}, (K_{19}^c)^{-1}, (K_{20}^c)^{-1}, (K_{21}^c)^{-1}, (K_{22}^c)^{-1}, (K_{23}^c)^{-1}, (K_{24}^c)^{-1}, \\
 & (K_{25}^c)^{-1}, (K_{26}^c)^{-1}, (K_{27}^c)^{-1}, (K_{28}^c)^{-1}, (K_{29}^c)^{-1}, (K_{30}^c)^{-1}, (K_{31}^c)^{-1}).
 \end{aligned}$$

Decryption round keys of the first, second, third and  $n$ -round associates with the encryption round keys as follows:

$$\begin{aligned}
 & (K_{32(i-1)}^d, K_{32(i-1)+1}^d, K_{32(i-1)+2}^d, K_{32(i-1)+3}^d, K_{32(i-1)+4}^d, K_{32(i-1)+5}^d, K_{32(i-1)+6}^d, K_{32(i-1)+7}^d, K_{32(i-1)+8}^d, \\
 & K_{32(i-1)+9}^d, K_{32(i-1)+10}^d, K_{32(i-1)+11}^d, K_{32(i-1)+12}^d, K_{32(i-1)+13}^d, K_{32(i-1)+14}^d, K_{32(i-1)+15}^d, K_{32(i-1)+16}^d, \\
 & K_{32(i-1)+17}^d, K_{32(i-1)+18}^d, K_{32(i-1)+19}^d, K_{32(i-1)+20}^d, K_{32(i-1)+21}^d, K_{32(i-1)+22}^d, K_{32(i-1)+23}^d, K_{32(i-1)+24}^d, \\
 & K_{32(i-1)+25}^d, K_{32(i-1)+26}^d, K_{32(i-1)+27}^d, K_{32(i-1)+28}^d, K_{32(i-1)+29}^d, K_{32(i-1)+30}^d, K_{32(i-1)+31}^d) \\
 = & (-K_{32(n-i+1)}^c, -K_{32(n-i+1)+1}^c, -K_{32(n-i+1)+2}^c, -K_{32(n-i+1)+3}^c, -K_{32(n-i+1)+4}^c, -K_{32(n-i+1)+5}^c, -K_{32(n-i+1)+6}^c, \\
 & -K_{32(n-i+1)+7}^c, -K_{32(n-i+1)+8}^c, -K_{32(n-i+1)+9}^c, -K_{32(n-i+1)+10}^c, -K_{32(n-i+1)+11}^c, -K_{32(n-i+1)+12}^c, \\
 & -K_{32(n-i+1)+13}^c, -K_{32(n-i+1)+14}^c, -K_{32(n-i+1)+15}^c, (K_{32(n-i+1)+16}^c)^{-1}, (K_{32(n-i+1)+14}^c)^{-1}, (K_{32(n-i+1)+18}^c)^{-1}, \\
 & (K_{32(n-i+1)+19}^c)^{-1}, (K_{32(n-i+1)+20}^c)^{-1}, (K_{32(n-i+1)+21}^c)^{-1}, (K_{32(n-i+1)+22}^c)^{-1}, (K_{32(n-i+1)+23}^c)^{-1}, \\
 & (K_{32(n-i+1)+24}^c)^{-1}, (K_{32(n-i+1)+25}^c)^{-1}, (K_{32(n-i+1)+26}^c)^{-1}, (K_{32(n-i+1)+27}^c)^{-1}, (K_{32(n-i+1)+28}^c)^{-1}, \\
 & (K_{32(n-i+1)+29}^c)^{-1}, (K_{32(n-i+1)+30}^c)^{-1}, (K_{32(n-i+1)+31}^c)^{-1}, i = \overline{1..n}.
 \end{aligned}$$

Decryption round keys applied to the first round and after the output transformation associated with the encryption round keys as follows:  $K_{32n+32+j}^d = K_{32n+64+j}^c$ ,  $K_{32n+64+j}^d = K_{32n+32+j}^c$ ,  $j = \overline{0..31}$ .

### 3 Results

Using the transformations SubBytes(), ShiftRows(), MixColumns() of the encryption algorithm AES as the round function network RFWKPES32-4 developed encryption algorithm AES-RFWKPES32-4. In the algorithm, the number of rounds of encryption and key's length is variable and the user can select the number of rounds and the key's length in dependence of the degree of secrecy of information and speed encryption.

As in the encryption algorithms based on the Feistel network, the advantages of the encryption algorithm AES-RFWKPES32-4 are that, when encryption and decryption process used the same algorithm. In the encryption algorithm AES-RFWKPES32-4 in decryption process encryption round keys are used in reverse order, thus on the basis of operations necessary to compute the inverse. For example, if the round key is multiplied by the subblock, while decryption is necessary to calculate the multiplicative inverse, if summarized, it is necessary to calculate the additive inverse.

It is known that the resistance of AES encryption algorithm is closely associated with resistance S-box, applied in the algorithm. In the S-box's encryption algorithm AES algebraic degree of nonlinearity  $\deg = 7$ , nonlinearity  $NL = 112$ , resistance to linear cryptanalysis  $\lambda = 32/256$ , resistance to differential cryptanalysis  $\delta = 4/256$ , strict avalanche criterion  $SAC = 8$ , bit independence criterion  $BIC = 8$ .

In the encryption algorithm AES-RFWKPES32-4 resistance S-box is equal to resistance S-box's encryption algorithm AES, i.e.,  $\deg = 7$ ,  $NL = 112$ ,  $\lambda = 32/256$ ,  $\delta = 4/256$ ,  $SAC = BIC = 8$ . These S-boxes are created based on Nyberg construction [1, 13].

Studies show that, speed of encryption encryption algorithms AES-RFWKPES32-4 higher than AES. The encryption algorithm AES-RFWKPES32-4 1.25 times encrypts faster than the AES.

### 4 Conclusions

It is known that as a algorithms based of Feistel network, the resistance algorithm based on networks RFWKPES32-4 closely associated with resistance round function. Therefore, selecting the transformations SubBytes(), ShiftRows(),



MixColumns() of the encryption algorithm AES, based on round function network RFWKPES32-4 we developed relatively resistant encryption algorithm.

## References

- [1] M. Aripov, G. Tuychiev, "About generation S-box size of 8x8," *Information Security in the Light of the Strategy Kazakhstan-2050: Proceedings of the I International Scientific and Practical Conference (September 12, 2013, Astana)*, pp. 116–125, 2013.
- [2] M. Aripov, G. Tuychiev, "Development block encryption algorithm based networks IDEA16-2 and RFWKIDEA16-2 using the transformation of encryption algorithm aes," *Information Security in the Light of the Strategy Kazakhstan-2050: Proceedings III International Scientific-practical Conference (15-16 October 2015, Astana)*, pp. 40–60, 2015.
- [3] J. Daeman, V. Rijmen, *AES Proposal: Rijndael, Version 2*, 1999. (<http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf>)
- [4] National Institute of Standards and Technology, *Announcing the Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197, 2001. (<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>)
- [5] G. Tuychiev, "About networks IDEA16-4, IDEA16-2, IDEA16-1, created on the basis of network IDEA16-8," *Compilation of Theses and Reports Republican Seminar Information Security in the Sphere Communication and Information. Problems and Their Solutions*, 2014.
- [6] G. Tuychiev, "About networks IDEA32-8, IDEA32-4, IDEA32-2, IDEA32-1, created on the basis of network IDEA32-16," *Infocommunications: Networks-Technologies-Solutions*, vol. 30, no. 2, pp. 45–50, 2014.
- [7] G. Tuychiev, "About networks IDEA8-2, IDEA8-1 and RFWKIDEA8-4, RFWKIDEA8-2, RFWKIDEA8-1 developed on the basis of network IDEA8-4," *Uzbek Mathematical Journal*, vol. 3, pp. 104–118, 2014.
- [8] G. Tuychiev, "About networks PES32-8, PES32-4, PES32-2 and PES32-1, created on the basis of network PES32-16," *Ukrainian Scientific Journal of Information Security*, vol. 20, issue 2, pp. 164–168, 2014.
- [9] G. Tuychiev, "About networks PES8-2 and PES8-1, developed on the basis of network PES8-4," *Transactions of the international scientific conference Modern problems of applied mathematics and information technologies-Al-Khorezmiy 2014*, vol. 2, pp. 28–32, 2014.
- [10] G. Tuychiev, "About networks RFWKIDEA16-8, RFWKIDEA16-4, RFWKIDEA16-2, RFWKIDEA16-1, created on the basis network IDEA16-8," *Ukrainian Scientific Journal of Information Security*, vol. 20, issue 3, pp. 259–263, 2014.
- [11] G. Tuychiev, "About networks rfwkPES32-8, rfwkPES32-4, rfwkPES32-2 and rfwkPES32-1," *Compilation of theses and reports republican seminar Information security in the sphere communication and information. Problems and their solutions*, 2014.
- [12] G. Tuychiev, "About networks rfwkPES8-4, rfwkPES8-2, rfwkPES8-1, developed on the basis of network PES8-4," *Transactions of the international scientific conference Modern problems of applied mathematics and information technologies-Al-Khorezmiy 2014*, vol. 2, pp. 32–36, 2014.
- [13] G. Tuychiev, "Generation of resistance boolean functions based on the nyberg construction and its application," *Information Security in the light of the Strategy Kazakhstan-2050: proceedings II International scientific-practical conference (15-17 October 2014, Astana)*, pp. 205–214, 2014.
- [14] G. Tuychiev, "New encryption algorithm based on network rfwkPES8-1 using of the transformations of the encryption algorithm aes," *International Journal of Multidisciplinary in Cryptology and Information Security*, vol. 3, no. 6, pp. 31–34, 2014.
- [15] G. Tuychiev, "About networks pes16-4, pes16-2 and pes16-1, created on the basis network pes16-8," *Ukrainian Information Security Research Journal*, vol. 17, no. 1, pp. 53–60, 2015.
- [16] G. Tuychiev, "About networks rfwkpes16-8, rfwkpes16-4, rfwkpes16-2 and rfwkpes16-1, created on the basis network pes16-8," *Ukrainian Information Security Research Journal*, vol. 17, no. 2, pp. 163–169, 2015.
- [17] G. Tuychiev, "About networks rfwkPES32-8, rfwkPES32-4, rfwkPES32-2 and rfwkPES32-1," *International Journal on Cryptography and Information Security (IJCIS)*, vol. 5, no. 1, pp. 9–20, 2015.
- [18] G. Tuychiev, "Creating a block encryption algorithm based networks PES32-1 and rfwkPES32-1 using transformation of the encryption algorithm aes," *Compilation scientific work scientific and practical conference Current issues of cyber security and information security-CICIS-2015*, pp. 101–112, 2015.
- [19] G. Tuychiev, "Creating a block encryption algorithm on the basis of networks IDEA32-4 and RFWKIDEA32-4 using transformation of the encryption algorithm aes," *Ukrainian Scientific Journal of Information Security*, vol. 21, issue 1, pp. 148–158, 2015.
- [20] G. Tuychiev, "The encryption algorithm aes-RFWKIDEA16-1," *Infocommunications: Networks-Technologies-Solutions*, no. 2 (34), pp. 48–54, 2015.

- [21] G. Tuychiev, "The encryption algorithm aes-RFWKIDEA32-1 based on network RFWKIDEA32-1," *Global Journal of Computer science and Technology: Network, Web and Security*, vol. 15, issue 4, pp. 33–41, 2015.
- [22] G. Tuychiev, "The encryption algorithms aes-pes16-1 and aes-rfwkpes16-1 based on networks pes16-1 and rfwkpes16-1," *International Journal of Electronics and Information Engineering*, vol. 3, no. 2, pp. 53–66, 2015.
- [23] G. Tuychiev, "The encryption algorithms aes-pes16-2 and aes-rfwkpes16-2," *Compilation of theses and reports republican seminar Information security in the sphere communication and information. Problems and their solutions*, 2015.
- [24] G. Tuychiev, "New encryption algorithm based on network IDEA16-1 using of the transformation of the encryption algorithm aes," *IPASJ International Journal of Information Technology*, no. 3, pp. 6–12, 2015.
- [25] G. Tuychiev, "New encryption algorithm based on network IDEA8-1 using of the transformation of the encryption algorithm aes," *IPASJ International Journal of Computer Science*, no. 3, pp. 1–6, 2015.
- [26] G. Tuychiev, "New encryption algorithm based on network PES8-1 using of the transformations of the encryption algorithm aes," *International Journal of Multidisciplinary in Cryptology and Information Security*, vol. 4, no. 1, pp. 1–5, 2015.
- [27] G. Tuychiev, "New encryption algorithm based on network RFWKIDEA8-1 using transformation of aes encryption algorithm," *International Journal of Computer Networks and Communications Security*, vol. 2, no. 3, pp. 43–47, 2015.
- [28] U.S. Department of Commerce/National Institute of Standards and Technology, *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication 46-3, 1979. (<http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>)

**Aripov Mirsaid** Doctor of Phys. Math. Science, Professor of National University of Uzbekistan.

**Tuychiev Gulom** candidate technical Sciences (Ph.D.), National University of Uzbekistan.

# A Note on “Efficient Algorithms for Secure Outsourcing of Bilinear Pairings”

Lihua Liu<sup>1</sup> and Zhengjun Cao<sup>2</sup>

(Corresponding author: Zhengjun Cao)

Department of Mathematics, Shanghai Maritime University<sup>1</sup>  
No.1550, Haigang Ave, Pudong New District, Shanghai, China

Department of Mathematics, Shanghai University<sup>2</sup>  
No.99, Shangda Road, Shanghai 200444, China

(Email: caozhj@shu.edu.cn)

(Received Mar. 13, 2016; revised and accepted May 20 & June 20, 2016)

## Abstract

Recently, Chen et al. have proposed a scheme [Theoretical Computer Science, 562 (2015), 112-121] for secure outsourcing of bilinear pairings. The scheme is motivated by the Chevallier-Mames et al.’s scheme. But the new scheme misses the feature of Chevallier-Mames et al.’s checking mechanism. In this note, we show that the verifying equations in the Chen et al.’s scheme cannot filter out some malformed values returned by the malicious servers, which makes it fragile to such malicious attacks. We also remark that the trick of equipping a low capability chip with two untrusted softwares in the scheme is somewhat artificial because of its heavy communication overhead.

*Keywords:* Bilinear Pairing; Outsourcing Computation; Semi-honest Server

## 1 Introduction

In 2000, Joux [19] proposed one round protocol for tripartite Diffie-Hellman key agreement protocol using Weil pairing. This is the first instance to show that pairings can be used for “good”. At Crypto’2001, Boneh and Fracklin [6] proposed a fully functional identity-based encryption scheme using Weil Pairing. After that, pairing-based cryptography (PBC) has interested many researchers [1, 2, 3, 4, 5, 7, 8, 9] because it has many beautiful and elegant properties.

Suppose that an elliptic curve  $E$  is defined over the finite field  $\mathbb{F}_q$ . Then elliptic curve cryptography (ECC) is working with elements which are defined over the base field  $\mathbb{F}_q$  (its parameters have size  $O(\log q)$  bits). But PBC is working with the functions and elements defined over the extension field  $\mathbb{F}_{q^k}$  (its parameters have size  $O(k \log q)$  bits), where  $k$  is the *embedding degree*. From the practical point of view, it is annoying for PBC schemes to have to work in extensions of the base fields, even though the inputting parameters are defined over the base field. The security of PBC depends directly on the intractable level of either elliptic curve discrete log problem (ECDLP) in the group  $E(\mathbb{F}_q)$  or discrete log problem (DLP) in the group  $\mathbb{F}_{q^k}^*$ . That means PBC protocols have to work in a running environment with parameters of 1024 bits so as to offer 80 bits security level [16].

The computation of bilinear pairing represents most of the computing cost when dealing with PBC protocols.

In order to mitigate the pairing computation burdens, researchers have put forth various methods. At Asi-crypt’05, Girault and Lefranc [15] introduced the primitive of server-aided verification to speed up the verification task of a signature scheme or an identification scheme. They assumed that the verifier has only small computation capabilities while having access to a more powerful, but untrusted server or, equivalently, to a trusted server via a non authenticated communication link.

At TCC’05, Hohenberger and Lysyanskaya [17] considered that an auxiliary server is made of two untrusted softwares which are assumed not to communicate with each other.

Liao and Hsiao [20] studied the problem of multi-servers aided verification using self-certified public keys for mobile clients. Liu et al. [22] have investigated the problem of identity-based server-aided decryption. Zhang and Sun [23] proposed an ID-based server-aided verification of short signature scheme without key escrow.

In 2013, Canard et al. [11] considered the method for generically transforming a given instance into a secure server-aided version. In 2014, Canard, Devigne and Sanders [10] provided some efficient ways to delegate the computation

of a pairing  $e(A, B)$ , depending on the status of  $A$  and  $B$ . Their protocols enable the limited device to verify the value received from the third party by computing one exponentiation.

In 2016, Cao et al. [12] pointed out two kinds of flaws in some server-aided verification schemes. Hsien et al. [18, 21] presented two surveys of public auditing for secure data storage in cloud computing.

Very recently, Chen et al. [13] have put forth a scheme for outsourcing computations of bilinear pairings in two untrusted programs model which was introduced by Hohenberger and Lysyanskaya [17]. In the scheme, a user  $T$  can indirectly compute the pairing  $e(A, B)$  by outsourcing some expensive work to two untrusted servers  $U_1$  and  $U_2$  such that  $A$ ,  $B$  and  $e(A, B)$  are kept secret. Using the returned values from  $U_1$ ,  $U_2$  and some previously stored values, the user  $T$  can recover  $e(A, B)$ .

The Chen et al.'s scheme is derived from the Chevallier-Mames et al.'s scheme [14] by storing some values in a table in order to save some expensive operations such as point multiplications and exponentiations. Besides, the new scheme introduces two servers  $U_1$  and  $U_2$  rather than the unique server  $U$  in the Chevallier-Mames et al.'s scheme. The authors [13] claim that the scheme achieves the security *as long as one of the two servers is honest*.

In other word, a malicious server cannot obtain either  $A$  or  $B$ . Unfortunately, the assumption cannot ensure that the scheme works well, because a malicious server can return some random values while the user  $T$  cannot detect the malicious behavior. As a result,  $T$  outputs a false value.

In this note, we show that the verifying equations in the Chen et al.'s scheme [13] cannot filter out some malformed values returned by the malicious servers. To fix this drawback, it has to specify that the servers are semi-honest. We also point out that the two untrusted programs model in the scheme is somewhat artificial and discuss some reasonable scenarios for outsourcing computations.

## 2 Review of the Scheme

Let  $\mathbb{G}_1$  and  $\mathbb{G}_2$  be two cyclic additive groups with a large prime order  $q$ . Let  $G_3$  be a cyclic multiplicative group of the same order  $q$ . A bilinear pairing is a map  $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow G_3$  with the following properties.

- 1) Bilinear:  $e(aR, bQ) = e(R, Q)^{ab}$  for all  $R \in \mathbb{G}_1$ ,  $Q \in \mathbb{G}_2$ , and  $a, b \in \mathbb{Z}_q^*$ .
- 2) Non-degenerate: There exist  $R \in \mathbb{G}_1$  and  $Q \in \mathbb{G}_2$  such that  $e(R, Q) \neq 1$ .
- 3) Computable: There is an efficient algorithm to compute  $e(R, Q)$  for all  $R \in \mathbb{G}_1$ ,  $Q \in \mathbb{G}_2$ .

The Chen et al.'s scheme [13] uses two untrusted servers  $U_1, U_2$ . The outsourcer  $T$  queries some pairings to the two servers. The scheme can be described as follows.

### Setup.

A trusted server computes a table *Rand* which consists of the elements of random and independent six-tuple

$$(W_1, W_2, w_1W_1, w_2W_1, w_2W_2, e(w_1W_1, w_2W_2)),$$

where  $w_1, w_2 \in_R \mathbb{Z}_q^*$ ,  $W_1 \in_R \mathbb{G}_1$ , and  $W_2 \in_R \mathbb{G}_2$ . The table is then loaded into the memory of  $T$ .

### Look-up table.

Given  $A \in \mathbb{G}_1$ ,  $B \in \mathbb{G}_2$ , where  $A$  and  $B$  may be secret or protected and  $e(A, B)$  is always secret or protected.  $T$  looks up *Rand* to create

$$\begin{aligned} & (V_1, V_2, v_1V_1, v_2V_1, v_2V_2, e(v_1V_1, v_2V_2)), \\ & (X_1, X_2, x_1X_1, x_2X_1, x_2X_2, e(x_1X_1, x_2X_2)), \\ & (Y_1, Y_2, y_1Y_1, y_2Y_1, y_2Y_2, e(y_1Y_1, y_2Y_2)). \end{aligned}$$

### Interaction with $U_1$ .

$T$  sends

$$(A + v_1V_1, B + v_2V_2), (v_1V_1 + v_2V_1, V_2), (x_1X_1, x_2X_2), (y_1Y_1, y_2Y_2)$$

to  $U_1$ .  $U_1$  returns

$$\begin{aligned} \alpha_1 &= e(A + v_1V_1, B + v_2V_2), \\ \delta &= e(V_1, V_2)^{v_1+v_2}, \\ \beta_1 &= e(x_1X_1, x_2X_2), \\ \beta_2 &= e(y_1Y_1, y_2Y_2). \end{aligned}$$

### Interaction with $U_2$ .

$T$  sends

$$(A + V_1, v_2 V_2), (v_1 V_1, B + V_2), (x_1 X_1, x_2 X_2), (y_1 Y_1, y_2 Y_2)$$

to  $U_2$ .  $U_2$  returns

$$\begin{aligned}\alpha_2 &= e(A + V_1, v_2 V_2), \\ \alpha_3 &= e(v_1 V_1, B + V_2), \\ \widehat{\beta}_1 &= e(x_1 X_1, x_2 X_2), \\ \widehat{\beta}_2 &= e(y_1 Y_1, y_2 Y_2).\end{aligned}$$

### Verification.

$T$  checks that both  $U_1$  and  $U_2$  produce the correct outputs by verifying that

$$\beta_1 = \widehat{\beta}_1 \text{ and } \beta_2 = \widehat{\beta}_2.$$

If not,  $T$  outputs “error”.

### Computation.

$T$  computes

$$e(A, B) = \alpha_1 \alpha_2^{-1} \alpha_3^{-1} \delta \cdot e(v_1 V_1, v_2 V_2)^{-1}.$$

**Remark 1.** In the original description of the scheme, the Step 2 (see Section 4.2 in Ref.[13]) has not specified any actions. It only explains that the pairing  $e(A, B)$  can be composed by the related values. The authors have confused the explanation with steps of the scheme (it is common that a step of a scheme should specify some actions performed by a participant), which makes the original description somewhat obscure.

**Remark 2.** It should be stressed that the pre-computation table must be very large in order to ensure the randomness of the picked tuples, which makes the proposed table-lookup method uncompetitive. Actually, it is a rare practice in cryptography to pick random numbers by table-lookup method.

## 3 The Checking Mechanism in the Scheme is Flawed

In the Chen et al.’s scheme [13], to check whether the returned values  $\alpha_1, \delta, \beta_1, \beta_2$  and  $\alpha_2, \alpha_3, \widehat{\beta}_1, \widehat{\beta}_2$  are properly formed, the user  $T$  has to check the verifying equations

$$\beta_1 = \widehat{\beta}_1 \text{ and } \beta_2 = \widehat{\beta}_2.$$

We now want to stress that the checking mechanism *cannot filter out some malformed values*. The drawback is due to that the protected values  $A, B$  are not involved in the equations at all.

For example, upon receiving

$$(A + v_1 V_1, B + v_2 V_2), (v_1 V_1 + v_2 V_1, V_2), (x_1 X_1, x_2 X_2), (y_1 Y_1, y_2 Y_2),$$

$U_1$  picks a random  $\rho \in \mathbb{Z}_q^*$  and returns

$$\alpha_1 = e(A + v_1 V_1, B + v_2 V_2), \rho, \beta_1 = e(x_1 X_1, x_2 X_2), \beta_2 = e(y_1 Y_1, y_2 Y_2)$$

to  $T$ .

Clearly,  $\beta_1 = \widehat{\beta}_1$  and  $\beta_2 = \widehat{\beta}_2$  hold still. Thus, the returned values will pass the verification process. But in such case, we have

$$\alpha_1 \alpha_2^{-1} \alpha_3^{-1} e(v_1 V_1, v_2 V_2))^{-1} \rho = e(A, B) e(V_1, V_2)^{-v_1 - v_2} \rho.$$

That means  $T$  obtains  $e(A, B) e(V_1, V_2)^{-v_1 - v_2} \rho$  instead of  $e(A, B)$ .

To fix the above drawback, we have to specify that *both two servers are semi-honest*. The term of semi-honest here means that a server can copy the involved values and always returns the correct outputs, but cannot conspire with the other server.

Under the reasonable assumption, the original scheme can be greatly simplified. We now present a revised version as follows.

**Look-up table.**

Given  $A \in \mathbb{G}_1, B \in \mathbb{G}_2$ , where  $A$  and  $B$  may be secret or protected and  $e(A, B)$  is always secret or protected.  
 $T$  looks up *Rand* to create

$$(V_1, V_2, v_1 V_1, v_2 V_1, v_2 V_2, e(v_1 V_1, v_2 V_2)).$$

**Interaction with  $U_1$ .**

$T$  sends

$$(A + v_1 V_1, B + v_2 V_2), (v_1 V_1 + v_2 V_1, V_2)$$

to  $U_1$ .  $U_1$  returns

$$\alpha_1 = e(A + v_1 V_1, B + v_2 V_2), \delta = e(V_1, V_2)^{v_1 + v_2}.$$

**Interaction with  $U_2$ .**

$T$  sends

$$(A + V_1, v_2 V_2), (v_1 V_1, B + V_2)$$

to  $U_2$ .  $U_2$  returns

$$\alpha_2 = e(A + V_1, v_2 V_2), \alpha_3 = e(v_1 V_1, B + V_2).$$

**Computation.**

$T$  computes

$$e(A, B) = \alpha_1 \alpha_2^{-1} \alpha_3^{-1} e(v_1 V_1, v_2 V_2)^{-1} \delta.$$

## 4 The Chevallier-Mames et al.'s Checking Mechanism

As we mentioned before, the Chen et al.'s scheme [13] is derived from the Chevallier-Mames et al.'s scheme [14]. But the new scheme misses the feature of the checking mechanism in the Chevallier-Mames et al.'s scheme. We think it is helpful for the later practitioners to explain the feature.

In the Chevallier-Mames et al.'s scheme, the outsourcer  $T$  wants to compute the pairing  $e(A, B)$  with the help of the untrusted server  $U$  such that  $A, B$  and  $e(A, B)$  are kept secret. The scheme can be described as follows (See Table 1).

Table 1: The Chevallier-Mames et al.'s scheme

The outsourcer $T$		The server $U$	
$\{P_1 \in \mathbb{G}_1, P_2 \in \mathbb{G}_2, e(P_1, P_2)\}$			
Input: $A \in \mathbb{G}_1, B \in \mathbb{G}_2$			
Pick $g_1, g_2, a_1, r_1, a_2, r_2 \in Z_q^*$ , compute $A + g_1 P_1, B + g_2 P_2$		Compute	
$a_1 A + r_1 P_1, a_2 B + r_2 P_2$	$\xrightarrow{(A+g_1 P_1, P_2)}$	$\alpha_1 = e(A + g_1 P_1, P_2)$	
and query them.	$\xrightarrow{(P_1, B+g_2 P_2)}$	$\alpha_2 = e(P_1, B + g_2 P_2)$	
	$\xrightarrow{(A+g_1 P_1, B+g_2 P_2)}$	$\alpha_3 = e(A + g_1 P_1, B + g_2 P_2)$	
Compute	$\xrightarrow{(a_1 A+r_1 P_1, a_2 B+r_2 P_2)}$	$\alpha_4 = e(a_1 A + r_1 P_1, a_2 B + r_2 P_2)$	
$e(A, B) = \alpha_1^{-g_2} \alpha_2^{-g_1} \alpha_3 e(P_1, P_2)^{g_1 g_2}$	$\xleftarrow{\alpha_1, \alpha_2, \alpha_3, \alpha_4}$	and return them.	
Check that			
$\alpha_4 \stackrel{?}{=} e(A, B)^{a_1 a_2} \alpha_1^{a_1 r_2} \alpha_2^{a_2 r_1}$ $\cdot e(P_1, P_2)^{r_1 r_2 - a_1 g_1 r_2 - a_2 g_2 r_1}$			
If true, output $e(A, B)$ .			

Notice that the true verifying equation is

$$\begin{aligned} \alpha_4 &= (\alpha_1^{-g_2} \alpha_2^{-g_1} \alpha_3 e(P_1, P_2)^{g_1 g_2})^{a_1 a_2} \cdot \alpha_1^{a_1 r_2} \alpha_2^{a_2 r_1} e(P_1, P_2)^{r_1 r_2 - a_1 g_1 r_2 - a_2 g_2 r_1} \\ &= \alpha_1^{-g_2 a_1 a_2 + a_1 r_2} \alpha_2^{-g_1 a_1 a_2 + a_2 r_1} \cdot \alpha_3^{a_1 a_2} e(P_1, P_2)^{g_1 g_2 a_1 a_2 + r_1 r_2 - a_1 g_1 r_2 - a_2 g_2 r_1} \end{aligned}$$

where  $\alpha_1, \alpha_2, \alpha_3, \alpha_4$  are generated by the server  $U$ , and the session keys  $g_1, g_2, a_1, r_1, a_2, r_2$  are randomly picked by the outsourcer  $T$ .



Clearly, the server  $U$  cannot generate the four-tuple  $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$  satisfying the above verifying equation because the exponents

$$a_1r_2 - g_2a_1a_2, a_2r_1 - g_1a_1a_2, a_1a_2, g_1g_2a_1a_2 + r_1r_2 - a_1g_1r_2 - a_2g_2r_1$$

are not known to the server. The intractability of the above equation can be reduced to the following general challenge:

Without knowing a secret exponent  $\theta$ , find  $X, Y \in Z_q^*$ ,  $X \neq 1, Y \neq 1$ , such that  $X^\theta = Y$ .

## 5 The Remote and Shared Servers

### 5.1 On the Client's Communication Overhead

The authors stress that the two servers  $U_1$  and  $U_2$ , in the real-world applications, can be viewed as two copies of one advertised software from two different vendors. We would like to remark that the two copies are neither nearby nor private. They must be remote and shared by many outsourcers. Otherwise, the user  $T$  equipped with two private copies of one software can be wholly viewed as an *augmented user*. But the situation is rarely considered in practice.

We now consider the situation that the outsourcer  $T$  has to communicate with two remote and shared servers. If the data transmitted over channels are not encrypted, then an adversary can obtain  $A + v_1V_1, B + v_2V_2$  by tapping the communication between  $T$  and  $U_1$ , and get  $v_1V_1, v_2V_2$  by tapping the communication between  $T$  and  $U_2$ . Hence, he can recover  $A$  and  $B$ . Thus, it is reasonable to assume that all data transmitted over channels are encrypted. From the practical point of view, the communication costs (including that of authentication of the exchanged data, the underlying encryption/decryption, etc.) could be far more than the computational gain in the scheme. The authors have neglected the comparisons between the computational gain and the incurred communication costs. Taking into account this drawback, we think the scheme is somewhat artificial.

### 5.2 A Nearby and Trusted Server

Girault and Lefranc [15] have described some situations in which a chip has only a small computation capability is connected to a powerful device.

- In a GSM mobile telephone, the more sensitive cryptographic operations are performed in the so-called SIM (Subscriber Identification Module), which is already aided by the handset chip, mainly to decipher the over-the-air enciphered conversation.
- In a payment transaction, a so-called SAM (Secure Access Module) is embedded in a terminal already containing a more powerful chip.
- A smart card is plugged into a personal computer, seeing that many PCs will be equipped with smart card readers in a near future.

We find that in all these situations (a SIM vs. a handset, a SAM vs. a powerful terminal, a smart card vs. a personal computer) the servers are nearby and trusted, not remote and untrusted.

## 6 Conclusion

The true goal of outsourcing computation in the Chen et al.'s scheme is to compute bilinear pairings. In view of that pairings spread everywhere in pairing-based cryptography, we do not think that the trick of equipping a low capability chip with two untrusted softwares is feasible because of its heavy communication overhead. In practice, we think, it is better to consider the scenario where a portable chip has access to a nearby and trusted server. Otherwise, the communication costs could overtake the computational gain of the outsourced computations.

## Acknowledgments

This work is supported by the National Natural Science Foundation of China (Project 61303200, 61411146001). The authors gratefully acknowledge the reviewers for their valuable suggestions.

## References

- [1] D. Boneh, "Pairing-based cryptography: Past, present, and future," in *Proceedings of Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security*, Beijing, China, December 2012.
- [2] D. Boneh and X. Boyen, "Short signatures without random oracles," *Journal of Cryptology*, vol. 21, no. 2, pp. 149–177, 2008.
- [3] D. Boneh and X. Boyen, "Efficient selective identity-based encryption without random oracles," *Journal of Cryptology*, vol. 24, no. 4, pp. 659–693, 2011.
- [4] D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *Proceedings of Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 440–456, Aarhus, Denmark, May 2005.
- [5] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proceedings of Advances in Cryptology - CRYPTO 2004, 24th Annual International Cryptology Conference*, pp. 41–55, Santa Barbara, California, USA, August 2004.
- [6] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proceedings of Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference*, pp. 213–229, Santa Barbara, California, USA, August 2001.
- [7] D. Boneh, A. Raghunathan, and G. Segev, "Function-private identity-based encryption: Hiding the function in functional encryption," in *Proceedings of Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security*, pp. 255–275, Bengaluru, India, December 2013.
- [8] D. Boneh, A. Raghunathan, and G. Segev, "Function-private subspace-membership encryption and its applications," in *Proceedings of Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference*, pp. 461–478, Santa Barbara, CA, USA, August 2013.
- [9] D. Boneh, A. Sahai, and B. Waters, "Fully collusion resistant traitor tracing with short ciphertexts and private keys," in *Proceedings of Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 573–592, St. Petersburg, Russia, 2006.
- [10] S. Canard, J. Devigne, and O. Sanders, "Delegating a pairing can be both secure and efficient," in *Proceedings of Applied Cryptography and Network Security - ACNS 2014*, pp. 549–565, Lausanne, Switzerland, June 2014.
- [11] S. Canard and et al., "Toward generic method for server-aided cryptography," in *Proceedings of Information and Communications Security - ICICS 2013*, pp. 373–392, Beijing, China, November 2013.
- [12] Z.J. Cao, L.H. Liu, and O. Markowitch, "On two kinds of flaws in some server-aided verification schemes," *International Journal of Network Security*, vol. 18, no. 6, pp. 1054–1059, 2016.
- [13] X.F. Chen and et al., "Efficient algorithms for secure outsourcing of bilinear pairings," *Theoretical Computer Science*, no. 562, pp. 112–121, 2015.
- [14] B. Chevallier-Mames and et al., "Secure delegation of elliptic-curve pairing," in *Proceedings of Smart Card Research and Advanced Application, 9th IFIP WG 8.8/11.2 International Conference - CARDIS 2010*, pp. 24–35, Passau, Germany, April 2010.
- [15] M. Girault and D. Lefranc, "Server-aided verification: Theory and practice," in *Proceedings of Advances in Cryptology - ASIACRYPT 2005*, pp. 605–623, Chennai, India, December 2005.
- [16] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. U.S.A: Springer-Verlag, 2004.
- [17] S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in *Proceedings of Theory of Cryptography - TCC 2005*, pp. 264–282, Cambridge, MA, USA, February 2005.
- [18] W.F. Hsien, C.C. Yang, and M.S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133–142, 2016.
- [19] A. Joux, "A one round protocol for tripartite diffie-hellman," in *Proceedings of Algorithmic Number Theory, 4th International Symposium, ANTS-IV*, pp. 385–394, Leiden, Netherlands, July 2000.
- [20] Y.P. Liao and C.M. Hsiao, "A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients," *Future Generation Computer Systems*, vol. 29, pp. 886–900, 2013.
- [21] C.W. Liu, W.F. Hsien, C.C. Yang, and M.S. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing," *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.
- [22] J. Liu, C.K. Chu, and J.Y. Zhou, "Identity-based server-aided decryption," in *Proceedings of Information Security and Privacy - ACISP 2011*, pp. 337–352, Melbourne, Australia, July 2011.
- [23] J.H. Zhang and Z.B. Sun, "An id-based server-aided verification short signature scheme avoid key escrow," *Journal of Information Science and Engineering*, vol. 29, pp. 459–473, 2013.



## Biography

**Lihua Liu** is an associate professor of Department of Mathematics at Shanghai Maritime University. She received her Ph.D. degree in applied mathematics from Shanghai Jiao Tong University. Her research interests include combinatorics, cryptography and information security.

**Zhengjun Cao** is an associate professor of Department of Mathematics at Shanghai University. He received his Ph.D. degree in applied mathematics from Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He served as a post-doctor in Computer Sciences Department, Université Libre de Bruxelles, from 2008 to 2010. His research interests include cryptography, discrete logarithms and quantum computation.

# Pixel Value Differencing Method Based on CMYK Colour Model

Shobana Manoharan, Deepika RajKumar

(Corresponding author: Shobana Manoharan)

Department of Electronics and Communication Engineering Karpagam College Of Engineering  
Coimbatore, Tamil Nadu, India

(Email: divyashobana.m@gmail.com)

(Received June 4, 2016; revised and accepted July 18 & July 24, 2016)

## Abstract

Due to tremendous improvements in the technology, all the confidential information are flying over the internet and most of the secured data are in the form of digital content. In this situation, data hiding techniques like Steganography stands in the position to protect the data in efficient manner from attackers. The style of embedding covert image over the cover image is termed as Image-Image Steganography. Here the methodology used for image-image steganography is modified form of pixel value differencing. Here, the secret image gets hidden in the cover object(image) in which the size of the message image is equivalent to the cover image and it is achieved by using CMYK colour model. Thus, the proposed algorithm provides a stego image with good quality measures and this algorithm is implemented with the help of matlab. Here the disturbance in the resultant image is calculated with the help of its PSNR and MSE values.

*Keywords: Data Hiding; Encoding Algorithm; Network Security; Steganography*

## 1 Introduction

Steganography is nothing but the approach of embedding and transmitting information via seemingly harmless covers in an attempt to obscure the presence of the message. The term "steganography" is an extract from Greek language, exactly means buried writing that comprises a huge array of approaches of covert communications that mask the presence of a secret object. Though steganography is an old skill, the commencement of computer technology has given it new birth. Computer based stenographic approaches announce alteration that covers medium to hide foreign data to the local carriers. That kind of message may be communicated in the form of text, binary files or produce extra information about the carrier and its authority such as digital watermarks or fingerprints. Steganography can be seen as cousin to cryptography. These two techniques have been used completely to insert elements of security to communication.

Cryptographic methods purposely disturb a message, so that, if it is interrupted, it cannot be cleared. This process is known as encryption and the encrypted message is termed as cipher text. Steganography in core "Camouflages", a message to skin its existence and make it seems unnoticed thus hiding the fact that a message is being sent in total. A cipher text message may capture attention while invisible messages will not [5].

One of the most popular cover objects used for steganography is an image. Cover images may be gray scale images or color images. Color images have large space for information hiding and therefore color image steganography is more popular than gray scale image steganography. Color images can be represented in various formats such as RGB (Red Green Blue), HSV, YUV, YIQ, YCbCr etc. Color image steganography can be done in any color space Domain [4].

Varieties of steganography is based on the kind of secret information gets embedded inside the cover medium. If the covert image gets hidden on the cover image then it is termed as Image steganography. If the message is text then it is called as text steganography and so on. Image steganography methods are broadly splitted into spatial domain based [3] and transform domain based methods [11] where the spatial domain hides the message bits in spatial intensity data by substitution and the transform domain techniques is used to hide the data on transform domain coefficients. Steganographic approaches are divided into 6 methods on the basis of the changes take place on the carrier medium. They are Transform domain, substitution, Statistics, Distortion, Spread spectrum and Cover generation based methods.

The Image-Image steganography based on Least Significant bits Substitution [9], Pixel Indicator [12] then Pixel Image intensity variation methods [10] need an image as the cover to hide the covert information which can be taken by altering the pixel values or by altering the intensity value of the pixel. The most common approach in the data hiding field is least-significant bits (LSBs) substitution where the fixed-length secret bits is embedded in the same fixed-length LSBs of pixels but it produces visible disturbance in the carrier medium. To minimize the disturbance led by LSBs substitution, several adaptive methods such as Optimal Pixel Adjustment Process [2] have been introduced. On the other hand, such adaptive methods differ from the others in the case of number of embedded bits in each pixel which owns good image quality [1]. Still, this can be attained by the capacity of lessening in the hiding capability.

## 2 Existing Method

The existing method is on the basis of pixel value differencing technique and modulus function. In the first step, the cover object is divided into Red, Green and Blue colour layers [6]. In this method, modulus function of 3 is applied to all the pixel value of the three colour planes. Let us consider the pixel value be  $p$ . The secret message is converted into base 3 digits. Let us consider this message value be  $m$ . During embedding process the value of  $p$  is compared to  $m$ . If the value of  $p$  is equal to  $m$ , then without any modification the cover pixel is considered as the stego pixel. If the value of  $p$  is greater than  $m$ , then increase the value of the cover pixel by 1 and that value is considered as a stego pixel. If the value of  $p$  is lesser than  $m$ , then decrease the value of the cover pixel by 1. This operation is carried out sequentially for all the three colour planes [7].

## 3 The Proposed Method

In this method, the cover image is splitted into cyan, magenta, yellow and black(key) colour for security purpose [8]. Because, most probably, all colour image steganography is based on red, green and blue layers. Here, modulus of 4 is applied for all pixel's value in the carrier image. By this, each cover pixel is capable of holding each pixel of message image. All pixels in the carrier image are involved in the process of embedding. The secret message is gray scale image and its size is equal to the cover image.

## 4 Algorithm

### 4.1 Embedding Method

Input: cover image(I), grayscale secret image(g);

Output: Stego image(s);

- 1) Convert RGB image to CMYK colour model.
- 2) Split the cover image in to cyan, magenta, yellow, and black layer (C, M, Y, K) respectively.
- 3) Take modulus function of 4 to all pixel values in the four layers as follows:

N be the number of pixels in the secret image;

For i =1 to N;

$$\text{C(i) mod 4} = \text{C1(i)};$$

$$\text{M(i) mod 4} = \text{M1(i)};$$

$$\text{Y(i) mod 4} = \text{Y1(i)};$$

$$\text{K(i) mod 4} = \text{K1(i)}.$$

- 4) Convert all pixel values of secret image to base 4 such that each pixel value is of digits as mentioned as follows:

$$(0)_{10} = (0000)_4(d1, d2, d3, d4)$$

$$(1)_{10} = (0001)_4(d1, d2, d3, d4)$$

$$\vdots \quad \quad \quad \vdots$$

$$(255)_{10} = (3333)_4(d1, d2, d3, d4).$$

- 5) The secret bit d1 will get embedded in C, d2 in M, d3 in Y and d4 in K. The Embedding process is carried out using Algorithm 1.
- 6) Convert the resultant image in to RGB image.

---

**Algorithm 1** EMBEDDING ALGORITHM
 

---

```

1: for  $j = 1$  to  $N$  do
2:   if  $C1[j] = d1[j]$  then
3:      $C[j] \leftarrow C[j]$ 
4:   else if  $C1[j] < d1[j]$  then
5:      $C[j] = \text{Function f1}(C1[j], d1)$ 
6:   else
7:      $C[j] = \text{Function f2}(C1[j], d1)$ 
8:   end if
9:   if  $M1[j] = d2[j]$  then
10:     $M[j] \leftarrow M[j]$ 
11:   else if  $M1[j] < d2[j]$  then
12:     $M[j] = \text{Function f1}(M1[j], d2)$ 
13:   else
14:     $M[j] = \text{Function f2}(M1[j], d2)$ 
15:   end if
16:   if  $Y1[j] = d3[j]$  then
17:     $Y[j] \leftarrow Y[j]$ 
18:   else if  $Y1[j] < d3[j]$  then
19:     $Y[j] = \text{Function f1}(Y1[j], d3)$ 
20:   else
21:     $Y[j] = \text{Function f2}(Y1[j], d3)$ 
22:   end if
23:   if  $K1[j] = d4[j]$  then
24:     $K[j] \leftarrow K[j]$ 
25:   else if  $K1[j] < d4[j]$  then
26:     $K[j] = \text{Function f1}(K1[j], d4)$ 
27:   else
28:     $K[j] = \text{Function f2}(K1[j], d4)$ 
29:   end if
30: end for

```

---

## 4.2 Functions Used in Embedding Algorithm

Here r1 is corresponding pixel sent to the following functions. It may be C, M, Y or K.

```

Function f1(r1,d)
If(r1 == 1)
    r1 = r1 + 1;
If(r1 == 2)
    r1 = r1 + 2;
If(r1 == 3)
    r1 = r1 + 3;
End
End

```

```

Function f2(r1,d)
If(r1 == 0)
    r1 = r1 - 3;
If(r1 == 1)
    r1 = r1 - 2;
If(r1 == 2)

```

```

    r1 = r1 - 1;
End
End

```

### 4.3 Extraction Method

Input: Stego image (S);

Output: Message image (g);

- 1) Convert Stego image from the RGB layers into CMYK colour layers.
- 2) Split the stego image into cyan, magenta, yellow, and black layer (C, M, Y, K respectively).
- 3) Take modulus function of 4 to all pixel values in the four layers and store it in separate array as A.
- 4) Split the array A such that each sub array equals to 4 digits.
- 5) Convert all 4 digits value in to its equivalent decimal value.
- 6) Arrange all the decimal value in sequential manner to form secret image(g).

## 5 Results and Discussions

In this method, for embedding purpose four Cover images were used. They are Lena, Gandhi, Mother Teresa and temple. Secret image is Baboon. Both of the secret image and cover image size is  $256 \times 256$ . The disturbance in the Stego image is calculated using PSNR and MSE. Let M and N be the rows and columns of the matrix of the image's pixels and R be the maximum error occurs in the stego image. Table 1 describes the PSNR and MSE values for the four stego images which are obtained with the help of proposed embedding algorithm. Figure 1 is the Secret image which is hidden in the cover images. Figures 2, 4, 6, 8 are the cover images used for embedding. Figures 3, 5, 7, 9 are the stego images. Figures 10, 12, 14, 16 are the histograms of the original images (Figures 2, 4, 6, 8 respectively). Figures 11, 13, 15, 17 are the histogram of the stego images (Figures 3, 5, 7, 9 respectively.)

Table 1: The MSE and PSNR values for the proposed method

Stego-Image	Red -PSNR	Red-MSE	Green-PSNR	Green-MSE	Blue-PSNR	Blue-MSE
<i>Lena</i>	60.3030	0.0606	58.9794	0.0822	60.1428	0.0629
<i>Gandhi</i>	60.2606	0.0612	55.9256	0.1662	56.1500	0.1578
<i>Mother Teresa</i>	57.9897	0.1033	56.6041	0.1421	58.4761	0.0924
<i>Temple</i>	58.7836	0.0860	57.4020	0.1183	59.8987	0.0666



Figure 1: Secret image (Baboon)



Figure 2: Cover Image (Lena)



Figure 3: Stego Image (Lena)

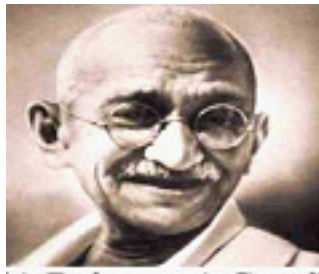


Figure 4: Cover Image (Gandhi)

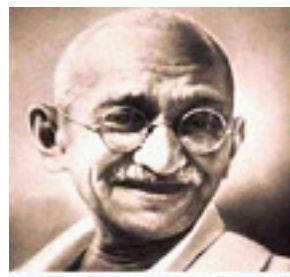


Figure 5: Stego Image (Gandhi)





Figure 6: Cover Image (Mother Teresa)



Figure 7: Stego Image (Mother Teresa)



Figure 8: Cover Image (Temple)



Figure 9: Stego image (Temple)

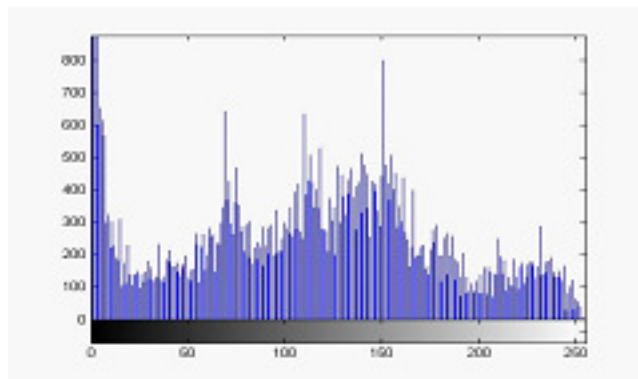


Figure 10: Histogram of CoverImage (Lena)

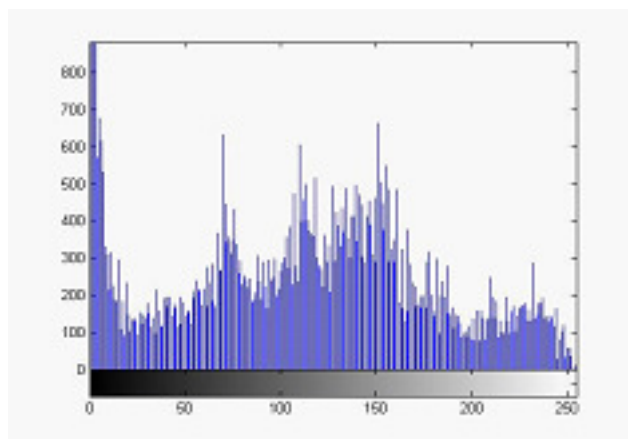


Figure 11: Histogram of Stego Image (Lena)

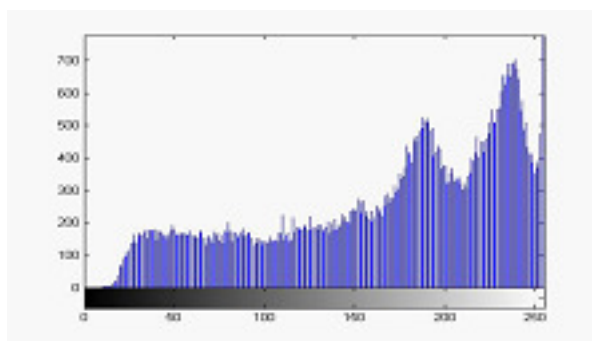


Figure 12: Histogram of CoverImage (Gandhi)

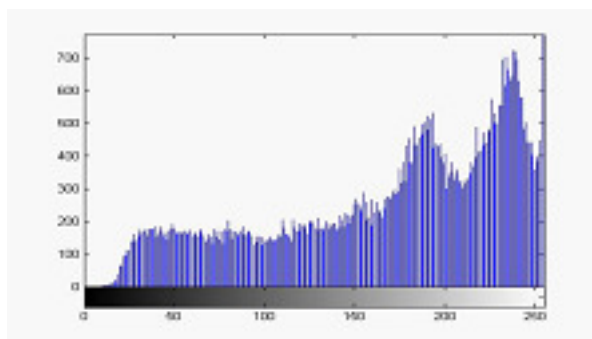


Figure 13: Histogram of Stego Image (Gandhi)

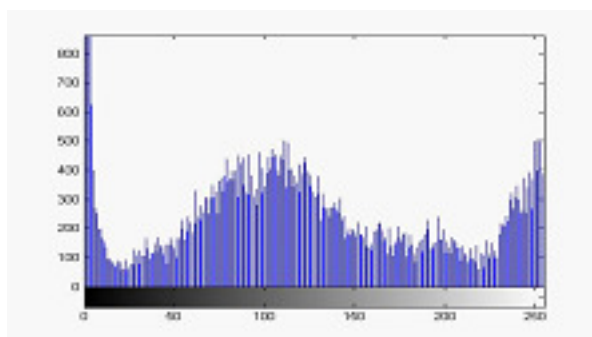


Figure 14: Histogram of Cover Image (Mother Teresa)

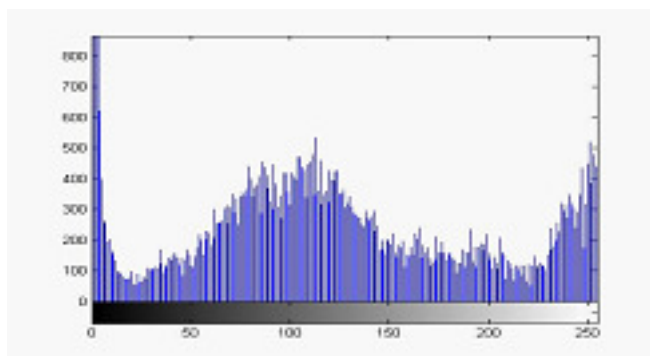


Figure 15: Histogram of Stego Image (Mother Teresa)

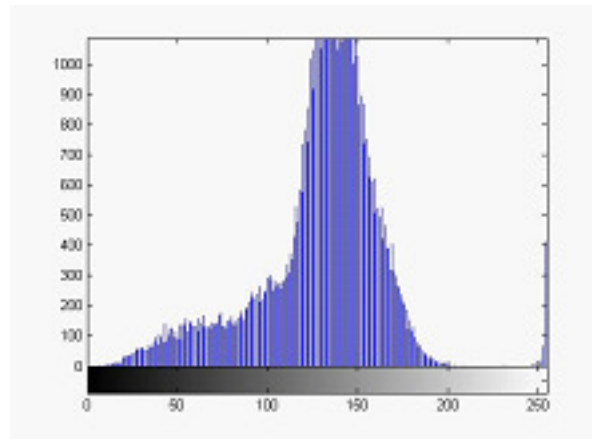


Figure 16: Histogram of Cover Image (Temple)

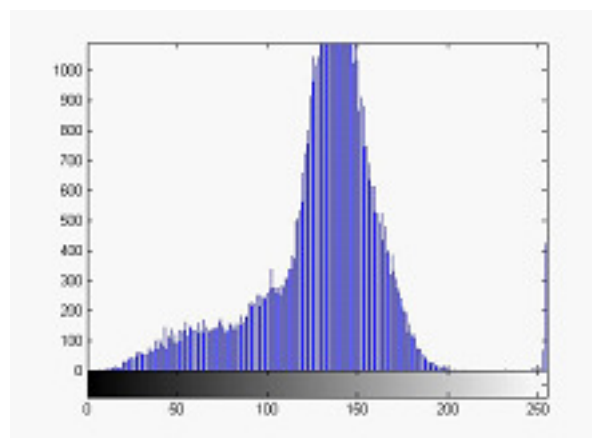


Figure 17: Histogram of Stego Image (Temple)

## 6 Conclusion

A new way of hiding technique has been proposed by introducing the concept of CMYK colour layers in image in the field of steganography. Hiding the message in CMYK colour layers provides more secure and good image quality rather than its RGB colour layers. The PSNR and MSE value is in good range in the CMYK approach when compared to RGB colour model. In this method, if the attacker tries to break the image into RGB colour layers also he cannot retrieve the message fully.

## References

- [1] R. Amirtharajan, D. Adarsh, V. Vignesh, and R. Boscobalaguru, "PVD blend with pixel indicator - OPAP composite for high fidelity steganography," *International Journal of Computer Application*, vol. 7, no. 9, p. 31?37, 2010.
- [2] C. K. Chan And L. M. Chen, "Hiding data in images by simple LSB substitution," *Pattern Recognition*, vol. 37, no. 8, pp. 469–474, 2004.
- [3] A. Cheddad, J. Condell, K. Curran, and P. Mckevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.
- [4] S. Hemalatha, U. Dinesh Acharya, and A. Renuka, "Wavelet transform based steganography technique to hide audio signals in image," *Procedia Computer Science*, vol. 47, no. 2, pp. 272–281, 2015.
- [5] S. Manoharan, "Efficient x-box mapping in stego-image using four-bit concatenation," *International Journal of Electronics and Information Engineering*, vol. 1, no. 1, pp. 29–33, 2014.
- [6] K. Muhammad, H. Farman, and M. Sajjad, "A secure method for color image steganography using gray-level modification and multi-level encryption," *KSII Transactions on Internet and Information Systems*, vol. 1, no. 10, pp. 27–32, 2015.
- [7] V. Nagaraj, Z. Dr Vijayalakshmi, and G. Dr Zayaraz, "Colorimage steganography based on pixel value modification method using modulus function," *IERI Procedia*, vol. 4, no. 11, pp. 17–24, 2013.
- [8] M. Shobana, "An efficient image steganographic algorithm using cmyk color model," *International Journal of Research and Innovations in Science & Technology*, vol. 90, no. 12, pp. 25–31, 2015.
- [9] M. Shobana, P. Gitanjali, M. Rajesh, and R. Manikandan, "A novel approach for hiding image using pixel intensity," *International Review on Computers and Softwares*, vol. 8, no. 5, pp. 904–908, 2013.
- [10] V. Thanikaiselvan, S. Kumar, N. Neelima, And R. Amirtharajan, "Data battle on the digital field between horse cavalry and interlopers," *Journal of Theoretical Technology*, vol. 29, no. 7, pp. 85–91, 2011.
- [11] Z. Thanikaiselvan, P. Arulmozhivarman, R. Amirtharajan, and J. B. BalaguruRayappan, "Wave (let) decide choosy pixel embedding for stego," in *IEEE 2011 International Conference on Computer, Communication and Electrical Technology*, pp. 157–162, 2011.
- [12] K. C. Wu, "Steganography using reversible texture synthesis," *IEEE Transactions on Image Processing*, vol. 24, no. 6, pp. 130–139, 2015.

## Biography

**M. Shobana** is working as an Assistant Professor in the Department of Electronics and Communication Engineering in Karpagam College of Engineering Tamil Nadu, India. Her area of interest is Steganography, Internet of Things and network Security.

**R. Deepika** is working as an Assistant Professor in the Department of Electronics and Communication Engineering at Karpagam College of Engineering Tamil Nadu, India. Her area of interest is Network On Chip, Steganography and network Security.

# Selecting Internet Videos and Pictures for Personalized Reminiscence Therapy

Hui-Wen Chien, Shu-Chuan Liao, Song-Lin Huang, Ching-Mao Chang,  
Hui-Ling Chen and Hsueh-Ting Chu

(Corresponding author: Hsueh-Ting Chu)

Department of Computer Science & Information Engineering, Asia University  
500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan  
(Email: htchu@asia.edu.tw)

(Received July 14, 2016; revised and accepted Aug. 18 & Aug. 30, 2016)

## Abstract

Dementia is the name for a group of symptoms caused by disorders that affect human brain. It is not a specific disease. Memory loss is most common symptom for dementia sufferers. Dementia is currently cannot be cured. Medicine can only prevent symptoms getting worse for a period of time. Instead of medication, reminiscence therapy is seen as an effective method for increasing self-esteem and emotional stability for people with dementia. Therefore, different forms of therapy try to recall the past life of the individual with the aim to keep the patient maintain thinking for mental health. This study discusses how to collect videos and pictures for personalized reminiscence therapy. There are millions of online videos and photos at different websites. However, there are two challenges to use these multimedia resources. First is how to avoid copyright infringement. Second is how to choose suitable resources for a patient. We contribute to the effectiveness of reminiscence therapy by enriching the content of reminiscence. Finally, our suggestion needs further research and feedback from practices of reminiscence intervention.

*Keywords: Dementia; Fair Use; Internet Video; Reminiscence Therapy*

## 1 Introduction

The world is ageing rapidly. People aged 60 and older make up 12.3 % of the global population, and by 2050, that number will rise to almost 22 per cent [20]. Rapid population aging and the average life expectancy cause the issues of long-term care, especially for people with dementia which is a broad category of brain diseases. It gradually causes a long term decrease in the ability to speak and think. People with dementia loss short-term memory and it affects their activities of daily living. There are four common types of dementia including Alzheimer's disease (50% 70%), vascular dementia (25%), Lewy body dementia (15%), and frontotemporal dementia [6].

Currently, no medications have been proved to prevent or cure dementia [17]. There are a lot of alternative therapies for integrative medicine of dementia such as acupuncture treatment [15, 18, 25] and aromatherapy [2, 16, 23]. Moreover, reminiscence therapy and music therapy are popular psychosocial interventions in dementia care, and reminiscence therapy is highly recognized by physicians [7, 8, 11, 12, 13, 22, 24]. Its effects on mood and cognition in dementia are less well understood [21].

The effectiveness of reminiscence therapy involves two factors. One is the prompt of some visual reminders such as photographs, household and other familiar items from the past, music and archive sound recordings [21]. The other is the conversation about the past story in the memory. It is critical what kind of visual reminders can trigger the recall of a dementia sufferer's past story. A newborn baby doll is useful for female patient [3, 5]. Similarly, effective reminiscence therapy also benefits from a reminiscence room decorated with objects from the past [4]. In this study, we investigate the usage of Internet videos and pictures for the purpose.



## 2 Group Reminiscence Therapy Versus Personized Reminiscence Therapy

Reminiscence therapy (RT) provides a means of helping participants to keeping his brain active. There are two major intervention types: group or individual [9]. Some researches combined both group and individual intervention types. The benefit of group reminiscence therapy is more audiences and the listening to patient narrative improves clinical care [10]. On the contrary, individual reminiscence therapy focused on personized intervention. People with dementia have their own life stories. Therefore, we aim to find Internet videos and pictures which can be linked to individual life stories to recall his memory to talk with the caregivers.

For the reason, we try to find visual objects according some criteria such as:

- 1) Where was his kindergarten or elementary school?
- 2) Where was his childhood playgrounds?
- 3) Where was his wedding place?
- 4) What are his favorite old TV series?
- 5) Who are his favorite old singers?
- 6) What kind of puppy did he have?
- 7) Who are his favorite old TV stars?
- 8) What are his favorite old songs?

For the collection of Internet videos and pictures, the copyright of multimedia materials is a critical issue in our design. As a result, we don't download any Internet resources and make use of the resources online.

## 3 Design of Personized Reminiscence Material

The best reminiscence resource is the collection of old pictures or items from the dementia sufferer's family. And it is better to encourage the family member to participate in the design of personized reminiscence materials. Figure 1. demonstrates a video of family reminiscence therapy made by a multimedia company. However, the number of old family pictures is usually limited for an individual person. It is necessary to collect more materials for reminiscence therapy. Thus, some of Internet videos and pictures can be applied to attract elders' interested and are hopeful to become subjects of discussion for reminiscence therapy.

### 3.1 Using Online Video Hosting Services

There are many videos hosting websites, such as YouTube and Youku that allows individuals to upload and share personal, business, or royalty-free videos and to watch them legally. Copyright is an important topic for using the videos. On the YouTube platform or the others, people can send a request to the video websites for claiming a copyright infringement and the removal of an unauthorized use. We have to restrict the use of online multimedia material with the concept of "fair use." Then we can only watch online videos without getting permission from the copyright owner.

Figure 2 lists the approximate numbers of old-time videos on the YouTube website. There are 30 40 thousands of videos in Chinese for each past decades. There are many clips uploaded by people made by old pictures. Besides, a massive amount of old documentaries, old movies and old TV series are available as well. We also emphasis the selection of MTV videos. On YouTube, the MTV of the film song "A Little Luck" ("Xiao Xing Yun" in Chinese) received more than one hundred million views within one year (Aug, 2015 Aug, 2016). The MTV is about the love story of an ordinary schoolgirl in 90's. It's so touchable because the viewers will recall their similar young story. Some of dementia sufferers are probably interested in such MTV clips because of keeping the memory of young or childhood affectional events.



Figure 1: A reminiscence video on YouTube made up of old pictures of a patient.

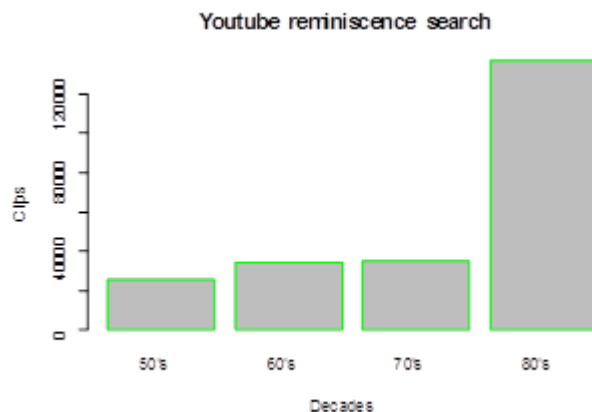


Figure 2: Search result of Old-time videos from the 1950s to the 1980s.


YouTube

TW


楚留香

篩選器


約 29,700 項結果




**楚留香 (1979年電視劇《楚留香》主題曲)**  
Song Old  
2 年前 · 觀看次數：846,954  
楚留香 (1979年電視劇《楚留香》主題曲) 作曲：顧嘉輝，填詞：鄧偉雄、黃霑，演唱：鄭少秋。



**1979年古裝連續劇(楚留香)**  
張發宗  
楚留香 (1979年電視劇《楚留香》主題曲) 3:20  
鄭少秋 楚留香 3:19  
查看完整播放清單 (35 部影片)



**《楚留香新傳》——(張智堯、樊少皇、金巧巧、劉德凱、傅藝偉)【38 集完結】**  
星光卫视官方頻道  
楚留香新傳 第01集 (張智堯、樊少皇、金巧巧、劉德凱、傅藝偉) 44:39  
楚留香新傳 第02集 (張智堯、樊少皇、金巧巧、劉德凱、傅藝偉) 44:59  
查看完整播放清單 (38 部影片)



**新楚留香**  
使用者 Google  
新楚留香 第1集 (任賢齊版) 47:16  
新楚留香 第2集 49:35  
查看完整播放清單 (40 部影片)

Figure 3: An example of interactive search for a patient's favorite videos. It's the result of searching "Chor Lau-heung" videos from YouTube.

3.2 Interactive Selecting Videos Using the YouTube Search Engine

In order to find out what are interesting to those dementia sufferers, we use a tablet to prompt the videos from the search interface of YouTube. And the caregiver inquires the elders about their favorite videos and records the search history as a personalized profile.

From the personalized profile, we can combine different videos into playlists. On the other hand, we can prepare talking topics for the playlist. For example, Chor Lau-heung is a Hong Kong television series in 1979 (Figure 3). During 1982, most of people in Taiwan watched an episode each weekend. We can bring an elder back to the old time to discuss who lived with him or her or which school his children studied. We can also investigate more videos during the interactive talk.

3.3 Build a Video From Old Photos

We can turn a series of old pictures into a video if the pictures are available from the dementia sufferer’s family. Or we can use the Google image search engine to collect old pictures (Figure 4). However, not all Internet pictures are royalty-free and it must be careful to get rid of copyright-protected pictures. The setting of usage right can filter only royalty-free pictures (Figure 5). There are web photo albums of old pictures which are open for use. Table 1. lists photo albums collected old pictures photographed in Taiwan during 50’s to 70’s.

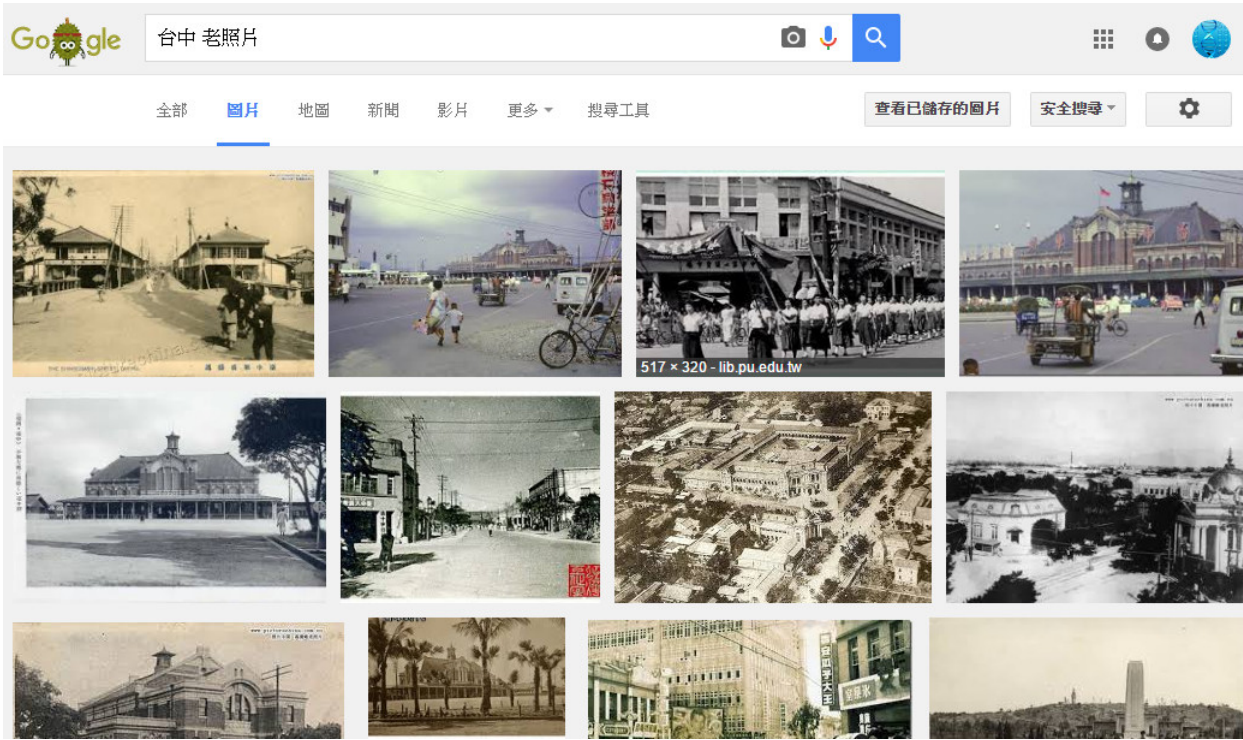


Figure 4: Test results of service response time

Table 1: Web photo albums of old Taiwan pictures

Photographer	Descriptions	URL
Tom Jones	1957-58 Taiwan	<a href="http://goo.gl/JsTNHw">http://goo.gl/JsTNHw</a>
Kevin Kelly	Taiwan 1972	<a href="https://goo.gl/15iyIw">https://goo.gl/15iyIw</a>
Casey Comer	1966-taichung-taiwan	<a href="http://goo.gl/sEZSB8">http://goo.gl/sEZSB8</a>



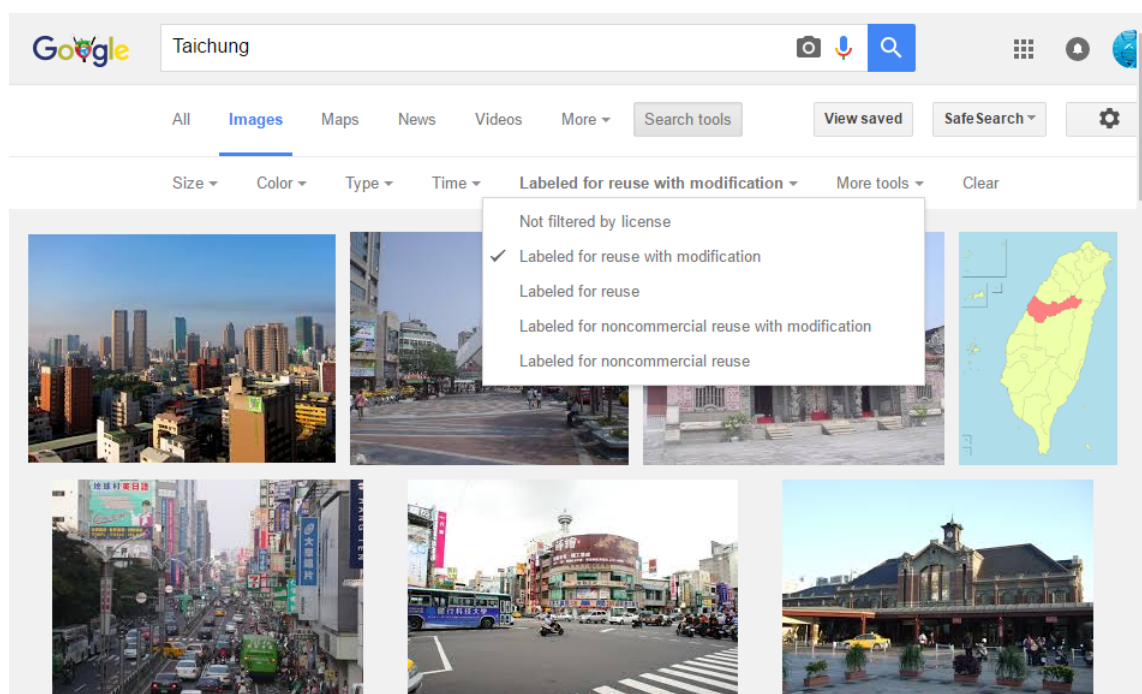


Figure 5: Setting of usage right in the Google image search engine including (1) Labeled for reuse (2) Labeled for reuse with modification (3) Labeled for noncommercial reuse (4) Labeled for noncommercial reuse with modification.

### 3.4 Narrative Reminiscence on Happiness

The intervention of reminiscence therapy is to let the patient feel joyful. Person with dementia can try to construct a narrative structure for the past story from the reminiscence linkages. Thus, reminiscence therapy can increase the positive emotions for elderly [24].

## 4 Advance Designs of Personalized Reminiscence

### 4.1 Personalized Reminiscence with Companion Robot

The ongoing development of robotics has relieved the limited application in industrial environments and more and more personal home robots been produced such as Asus zenbo and Softbank Pepper (Figure 6). Pepper is a humanoid robot and Zenbo is more like an animaloid. Both are designed for multiple purposes. One big application is to play the role of companion robot for children or elders. Today, most of countries in the world are facing ageing population, at the same time more elderly individuals are suffering from dementia. It raises the demand to apply companion robots to improve the quality of care for persons with dementia [1, 14]. Therefore, companion robots can be added a design of personalized reminiscence profile for elderly. Consequently, they can play personalized videos or music during the companion of a dementia sufferer or other elders.

### 4.2 Make Old-time TV or Radio Player

The decoration of a reminiscence room with nostalgic items may help dementia sufferers feeling more easily into memories from their past. Therefore, we can reconstruct nostalgic TV set by inserting a new all-in-one computer into a case of old TV set for playing old videos (Figure 7A). Similarly, we can reconstruct nostalgic radio player by inserting a new mp3 player into a case of old stereo for playing old songs (Figure 7B).

## 5 Conclusions

Reminiscence therapy has been recognized as an independent nursing intervention by American nursing association [19]. This study discussed the usage of Internet videos and pictures for personalized reminiscence therapy.

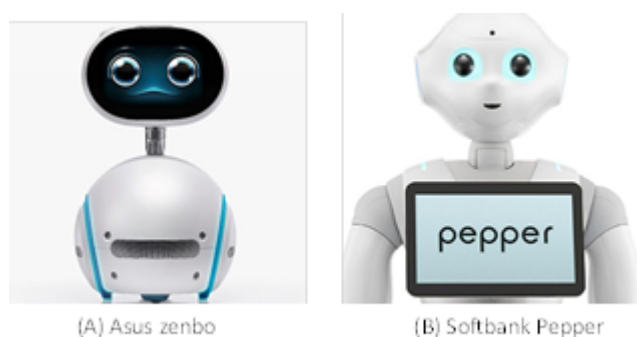


Figure 6: Concept of education cloud for the access of learning contents from different terminal devices.

Currently, the evidence of outcome from reminiscence therapy is still limited. It is important to collect more cases of reminiscence therapy which can be shared with other care institutions.

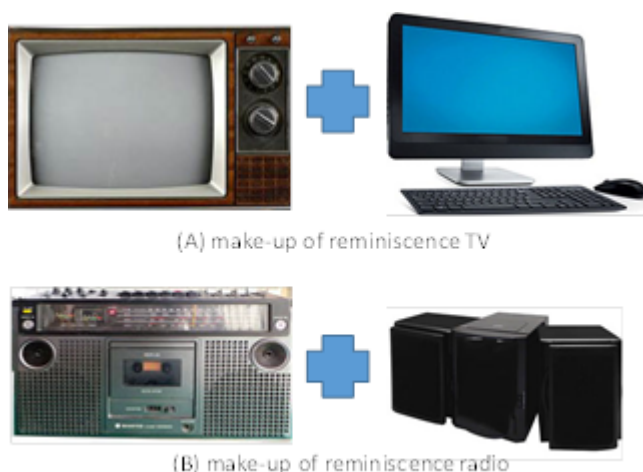


Figure 7: Make old-time TV or radio player for the decoration of a reminiscence room

## Acknowledgment

The authors are grateful to the generous supports from Asia University. This research is supported by the Ministry of Science and Technology, Taiwan under Grant no. 105-2410-H-468-025.

## References

- [1] R. Bemelmans, G. J. Gelderblom, P. Jonker, and L. de Witte, "Socially assistive robots in elderly care: a systematic review into effects and effectiveness," *Journal of Am Med Dir Assoc*, vol. 13, pp. 114–120, Feb. 2012.
- [2] C. Bilien, N. Depas, G. Delaporte, and N. Baptiste, "Benefits of aromatherapy in dementia special care units," *Soins Gerontol*, pp. 35–40, May-June 2016.
- [3] L. Bisiani and J. Angus, "Doll therapy: A therapeutic means to meet past attachment needs and diminish behaviours of concern in a person living with dementia—a case study approach," *Dementia (London)*, vol. 12, pp. 447–62, July 2013.
- [4] P. Boersma, J. C. van Weert, B. van Meijel, and R. M. Droes, "Implementation of the veder contact method in daily nursing home care for people with dementia: A process analysis according to the re-aim framework," *Journal of Clin Nurs*, June 2016.
- [5] B. A. Braden and P. M. Gaspar, "Implementation of a baby doll therapy protocol for people with dementia: Innovative practice," *Dementia (London)*, vol. 14, pp. 696–706, Sep 2015.



- [6] A. Burns and S. Iliffe, "Dementia," *British Medical Journal*, vol. 338, pp. b75, 2009.
- [7] G. Charlesworth, K. Burnell, N. Crellin, Z. Hoare, J. Hoe, M. Knapp, et al., "Peer support and reminiscence therapy for people with dementia and their family carers: A factorial pragmatic randomised trial," *Journal of Neurol Neurosurg Psychiatry*, 2016.
- [8] S. M. Chen, C. L. Kuo, M. R. Chen, L. L. Lee, P. Y. Lee, and S. F. Wang, "The effect of structured group reminiscence therapy on the life satisfaction of institutionalized elderly," *Hu Li Za Zhi*, vol. 63, pp. 70–79, Aug. 2016.
- [9] R. Cheston and A. Ivanecka, "Individual and group psychotherapy with people diagnosed with dementia: a systematic review of the literature," *International Journal of Geriatr Psychiatry*, July 2016.
- [10] J. Clark, "The narrative in patient-centred care," *The British Journal of General Practice*, vol. 58, pp. 896–896, 2008.
- [11] D. J. Hallford and D. Mellor, "Brief reminiscence activities improve state well-being and self-concept in young adults: A randomised controlled experiment," *Memory*, pp. 1–10, Nov. 2015.
- [12] D. J. Hallford and D. Mellor, "Autobiographical memory-based intervention for depressive symptoms in young adults: A randomized controlled trial of cognitive-reminiscence therapy," *Psychother Psychosom*, vol. 85, pp. 246–249, 2016.
- [13] U. Jonsson, G. Bertilsson, P. Allard, H. Gyllensvard, A. Soderlund, A. Tham, et al., "Psychological treatment of depression in people aged 65 years and over: A systematic review of efficacy, safety, and cost-effectiveness," *PLoS One*, vol. 11, pp. e0160859, 2016.
- [14] L. Odetti, G. Anerdi, M. P. Barbieri, D. Mazzei, E. Rizza, P. Dario, et al., "Preliminary experiments on the acceptability of animaloid companion robots by older people with early dementia," in *Proceedings of IEEE Eng Med Biol Soc*, vol. 2007, pp. 1816–9, 2007.
- [15] W. N. Peng, H. Zhao, Z. S. Liu, and S. Wang, "Acupuncture for vascular dementia," *Cochrane Database Syst Rev*, pp. Cd004987, 2007.
- [16] O. Press-Sandler, T. Freud, I. Volkov, R. Peleg, and Y. Press, "Aromatherapy for the treatment of patients with behavioral and psychological symptoms of dementia: A descriptive analysis of RCTs," *Journal of Altern Complement Med*, vol. 22, pp. 422–428, June 2016.
- [17] M. S. Rafii and P. S. Aisen, "Recent developments in Alzheimer's disease therapeutics," *BMC Medicine*, vol. 7, pp. 1–4, 2009.
- [18] G. X. Shi, Q. Q. Li, B. F. Yang, Y. Liu, L. P. Guan, M. M. Wu, et al., "Acupuncture for vascular dementia: A pragmatic randomized clinical trial," *Scientific World Journal*, vol. 2015, pp. 161439, 2015.
- [19] C. K. Stinson and E. Kirk, "Structured reminiscence: an intervention to decrease depression and increase self-transcendence in older women," *Journal of Clin Nurs*, vol. 15, pp. 208–218, Feb. 2006.
- [20] UNFPA, United Nations Population Fund Report, 2016. (<http://www.unfpa.org/ageing>)
- [21] B. Woods, A. Spector, C. Jones, M. Orrell, and S. Davies, "Reminiscence therapy for dementia," *Cochrane Database Syst Rev*, pp. Cd001120, 2005.
- [22] Y. P. Yang, F. P. Lee, H. C. Chao, F. Y. Hsu, and J. J. Wang, "Comparing the effects of cognitive stimulation, reminiscence, and aroma-massage on agitation and depressive mood in people with dementia," *Journal of Am Med Dir Assoc*, vol. 17, pp. 719–24, Aug. 2016.
- [23] Y. P. Yang, C. J. Wang, and J. J. Wang, "Effect of aromatherapy massage on agitation and depressive mood in individuals with dementia," *Journal of Gerontol Nurs*, pp. 1–9, 2016.
- [24] Z. Yousefi, K. Sharifi, Z. Tagharrobi, and H. Akbari, "The effect of narrative reminiscence on happiness of elderly women," *Iran Red Crescent Med Journal*, vol. 17, pp. e19612, Nov. 2015.
- [25] J. Yu, X. Zhang, C. Liu, Y. Meng, and J. Han, "Effect of acupuncture treatment on vascular dementia," *Neurol Res*, vol. 28, pp. 97–103, Jan. 2006.

## Biography

**Hui-Wen Chien**, RN (Taiwan & Australia) received her M.S (Gerontology) and Ph.D. degrees from The University of Sydney, Australia. She then joined the Department of Nursing, Asia University, Taichung. Her research interests include dementia care, health promotions, qualitative study, long-term care and care models.

**Shu-Chuan Liao** received her Ed.D. degrees from Northern Illinois University. She then joined the Department of Social Work, Asia University, Taichung. Her research interests include community work, group work, adult learning, service learning, care for the vulnerable population and research.

**Song-Lin Huang** received his Ph.D. degrees from Newcastle University. He joined the Department of Social work, Asia University, Taichung. His research interests include social gerontology and aging society.

**Ching-Mao Chang** is currently a M.D. in Taipei Veterans General Hospital and a Ph.D. candidate in Graduate Institute of Clinical Medicine, Chang Gung University. His research interests include Chinese medicine and autoimmune disease.

**Hui-Ling Chen** received her M.S. degrees from Northern Illinois University. She then joined the Department of Early Childhood Care and Education, University of Kang-Ning, Taipei. Her research interests include early childhood care and Eugenics.

**Hsueh-Ting Chu** received his M.S. and Ph.D. degrees from National Tsing Hwa University in 1997 and in 2002, both in Computer Science. He then joined the Department of Computer Science and Information Engineering, Asia University, Taichung. His research interests include bioinformatics, cloud computing, social networking and e-learning.

## **Guide for Authors**

### **International Journal of Electronics and Information Engineering**

International Journal of Electronics and Information Engineering (IJEIE) will be committed to the timely publication of very high-quality, peer-reviewed, original papers that advance the state-of-the art and applications of Electronics and Information Engineering. Topics will include, but not be limited to, the following: Algorithms, Bioinformatics, Computation Theory, AI, Fuzzy Systems, Embedded Systems, VLSI/EDA, Computer Networks, Information Security, Database, Data Mining, and Information Retrieval, Digital Content, Digital Life, and Human Computer Interaction, Image Processing, Computer Graphics, and Multimedia Technologies, Information Literacy, e-Learning, and Social Media, Mobile Computing, Wireless Communications, and Vehicular Technologies, Parallel, Peer-to-peer, Distributed, and Cloud Computing, Semiconductor, Software Engineering and Programming Languages, Telecommunication, etc.

#### **1. Submission Procedure**

Authors are strongly encouraged to submit their papers electronically by using online manuscript submission at <http://ijeie.jalaxy.com.tw/>.

#### **2. General**

Articles must be written in good English. Submission of an article implies that the work described has not been published previously, that it is not under consideration for publication elsewhere. It will not be published elsewhere in the same form, in English or in any other language, without the written consent of the Publisher.

##### **2.1 Length Limitation:**

All papers should be concisely written and be no longer than 30 double-spaced pages (12-point font, approximately 26 lines/page) including figures.

##### **2.2 Title page**

Title page should contain the article title, author(s) names and affiliations, address, an abstract not exceeding 100 words, and a list of three to five keywords.

##### **2.3 Corresponding author**

Clearly indicate who is willing to handle correspondence at all stages of refereeing and publication. Ensure that telephone and fax numbers (with country and area code) are provided in addition to the e-mail address and the complete postal address.

##### **2.4 References**

References should be listed alphabetically, in the same way as follows:

For a paper in a journal: M. S. Hwang, C. C. Chang, and K. F. Hwang, "An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445--446, 2002.

For a book: Dorothy E. R. Denning, *Cryptography and Data Security*. Massachusetts: Addison-Wesley, 1982.

For a paper in a proceeding: M. S. Hwang, C. C. Lee, and Y. L. Tang, "Two simple batch verifying multiple digital signatures," in *The Third International Conference on Information and Communication Security (ICICS2001)*, pp. 13--16, Xian, China, 2001.

In text, references should be indicated by [number].

##### **2.5 Author benefits**

No page charge is made.

## **Subscription Information**

Individual subscriptions to IJEIE are available at the annual rate of US\$ 200.00 or NT 6,000 (Taiwan). The rate is US\$1000.00 or NT 30,000 (Taiwan) for institutional subscriptions. Price includes surface postage, packing and handling charges worldwide. Please make your payment payable to "Jalaxy Technique Co., LTD." For detailed information, please refer to <http://ijeie.jalaxy.com.tw> or Email to [ijeieoffice@gmail.com](mailto:ijeieoffice@gmail.com).