IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 10, No. 5, October, 2020, pp. 655-661
Journal homepage: http://iieta.org/journals/ijsse

Image Encryption Based on Matrix Factorization

Vivek Khalane[1*], Shekhar Suralkar[2], Umesh Bhadade[3]

[1] Department pf Instrumentation Engineering, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai 00706, India
[2] Department of Electronics and Telecommunication Engineering, SSBT College of Engineering and Technology, Jalgaon 425001, Maharashtra, India
[3] Research Guide, Electronics Engineering, Kavayitri Bahinabai Chaudhari North Maharashtra University, Jalgaon 425001, Maharashtra, India

Corresponding Author Email: vivek.khalane@rait.ac.in

https://doi.org/10.18280/ijsse.100510

Received: 25 July 2020
Accepted: 16 October 2020

Keywords:
data security, image encryption, matrix decomposition, independent component analysis, non-negative matrix decomposition

ABSTRACT

In this paper, we present a matrix decomposition-based approach for image cryptography. The proposed method consists of decomposing the image into different component and scrambling the components to form the image encryption technique. We use two different type of matrix decomposition techniques to check the efficiency of proposed encryption method. The decomposition techniques used are Independent component analysis (ICA) and Non-Negative Matrix factorization (NMF). The proposed technique has unique user defined parameters (key) such as decomposition method, number of decomposition components and order in which the components are arranged. The unique encryption technique is designed on the basis of these key parameters. The original image can be reconstructed at the decryption end only if the selected parameters are known to the user. The design examples for both decomposition approaches are presented for illustration purpose. We analyze the complexity and encryption time of cryptography system. Results prove that the proposed scheme is more secure as it has less correlation between the input image and the encrypted version of the same as compared to state-of-art methods. The computation time of the proposed approach is found to be comparable.

1. INTRODUCTION

Due to the necessity of computerized right management for network system and multimedia, we transmit large number of images over internet and wireless network. Therefore, the image encryption technology has received great attention and many techniques have been developed for the same. Recently, multimedia disturbances suffer with issue like data management and cloud storage through the internet. Therefore, image encryption technique with the capability of secured access are required. Many researchers have proposed various encryption methods [1-3]. Linear dimensionality reduction (LDR) technique is used for data analysis in various application such as compression, registration, feature extraction and noise filtering. LDR optimize the approximation effectively by curtailing singular value decomposition (SVD) into three matrices where two unitary matrices factorized diagonal matrix [4-6]. The lower rank in diagonal matrix can be obtained by adding singular value in approximate image. SVD is same as principal component analysis (PCA) by centering all data points at origin. The resulting principal components in PCA are still dependent therefore the source isolation is not possible. Independent Component analysis (ICA) is a source separation technique in which independent signals taken into consideration for higher order correlation. For signal registration, analysis, compression and encryption purposes, a two-dimensional (2D) image decomposed into matrix components using several techniques like vector quantization (VQ) [7, 8], singular value decomposition (SVD) [9] and non-negative matrix factorization (NMF) [10-12]. The VQ method is help to reduce the computation complexity in image compression. In 1994, Paatero and topper invented the NMF algorithm and Lee and Seung further studied it. NMF can be expressed as nonnegative matrix, which is product of weighting vector and basis image. Both the collective matrix factorization (CMF) and homomorphic encryption (HE) design algorithm to facilitate the model without loss of any information by mapping the matrices for each unified feature vectors [13]. NMF model [14] is introduced three steps binarization framework for MS document images using three steps of features extraction, post processing methods and applying algorithm for selected coefficient parameter to extract the text. An efficient watermarking scheme has been proposed based on Hessenberg Matrix decomposition which transforming the cover image by discrete wavelet transform [15].

NMF techniques have been applied in various research area like micro array data analysis, molecule pattern analysis, collaborative filtering, bioinformatics, multimedia data. In some applications, the similarity index is found very high between original images and basis image. However, this is problem in image encryption because the attacker can quickly retrieve the original image from the basis image. To solve this problem, we have modified the encryption order of basis components. By doing image factorization using ICA/NMF, we decorrelate the input data and hence by doing that it improves data security (reduce correlation). This paper presents a new methodology for digital image encryption using two of these matrix/image decomposition techniques. The proposed method consists of decomposing the image into different component and scrambling the components to form the image encryption technique. The designed technique has various user defined parameters (key) like, decomposition method, number of decomposition components and order in which the components are arranged. Based on the selection of these parameters, we can design a unique image encryption technique. The rest of this paper is organized as follows: In Section II, we briefly review the basics of matrix decomposition techniques. In Section III, we present a proposed method for image cryptography using both the matrix decomposition techniques. Section IV, presents experimentation for the proposed method and results discussion and we conclude the paper in section.

2. PREVIEW OF MATRIX DECOMPOSITION TECHNIQUE

Matrix decomposition is methods which quantify given matrix by splitting a matrix into constituent parts. Matrix decomposition methods is known as matrix factorization methods which is the basis of linear algebra in computers science [16]. It helps to solve linear equation, reverse calculation and computation of the determinant of a matrix.

Lets **R** is size of |U|×|D|. Our aim is to find out two matrices **P** (a|U|×K matrix) and **Q** (a|D|×K matrix) so that the value is approximate to **R**.

$$R \approx P \times Q^T = \hat{R} \qquad (1)$$

where, **P** represents strong relationship between the features and user likewise **Q** represents strong relationship between the features and item. The rating of d_j using u_j calculated by taking dot product of vector corresponding to d_j and u_j.

$$\hat{r}_{i,j} = p_i^T q_j = \sum_{k=1}^{K} p_{i,k} q_{k,j} \qquad (2)$$

P and **Q** obtained by initializing some value in the matrices, calculate difference between their product is to M. and iteratively minimize the difference. This technique known as gradient decent.

2.1 Nonnegative Matrix Factorization

Non negative matrix factorization is used to find out basis image and weighting function from given matrix. Let the matrix **X** define approximate data matrix [17, 18]. NMF algorithm decomposing a given nonnegative data matrix **X** into weighting matrix **W** and basis matrix **H** as shown in Figure 1. Matrix **X** is approximated by a linear combination of column of weighting matrix **W** and basis matrix **H**.

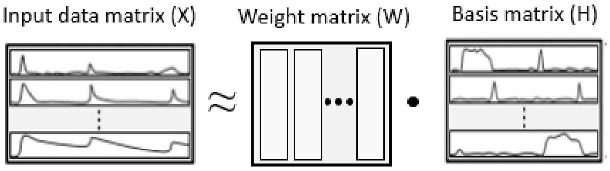

Figure 1. Non negative matrix factorization

The column of **X** is nonnegative matrix having *i* and *j* as dimensional data vectors and number of data vectors respectively.

$$x_i = \left[w_{i1} w_{i2} \cdots w_{ik} \right] \times \begin{bmatrix} h_1 \\ h_2 \\ \vdots \\ h_k \end{bmatrix} = \sum_{j=1}^{k} w_{ij} \times h_i \qquad (3)$$

This matrix **X** is approximately factorized into (*ik*) matrix W and (*kj*) matrix **H** where k is rank of factorization which is smaller than *i* and *j*. Therefore, total number in **X** is larger than number of coefficients in **W** and **H** (i.e. *ij+jk≤ik*). If we chose *k=i/j* then there is no loss. In our experimentation we have chosen *k=i* (no order reduction), Hence our technique is lossless. The new value of **W** and **H** is calculated at each iteration by recent value and factor that depend on the quality of approximation for representing original matrix. The accuracy of NMF algorithm improves monotonically with the application using multiplicative updates rule.

2.2 Independent Component Analysis

ICA is a way to decompose the data into its independent components. ICA solves the problem of recovering statically independent components from the input [19]. We have used ICA instead of SVD for following reasons.

- Complexity in interpretation can be reduced by utilizing few principal components that explain large proposition of total variation.
- ICA reduces dimensionality by rejecting lower variance components.
- ICA helps to remove the correlated variable in dataset to improve the performance of algorithm.
- Noise is reduced as maximum variation basis is chosen and minimum variation removes automatically in the background. Hence it increases robustness of encryption algorithm.
- In case of SVD, Input matrix is decomposed into three different matrices instead of two (in case of ICA). Hence there is increase in redundancy in case of SVD as compared to ICA.

ICA has drawback that, Standard dataset is required to avoid the biasing of features in data set so that calculated principal component avoid less information which leads to accurate result.

The objective of ICA is to estimate the basis source signals present in the original signal even if they are not all statically independent. Independence is better than uncorrelation as it evaluates reality of relation while uncorrelation determine only linear relationship. The pattern of ICA model is as below:

$$X = AS \qquad (4)$$

Same can be represented in matrix form as below:

$$\begin{bmatrix} x_1(t) \\ \vdots \\ x_N(t) \end{bmatrix} = \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{1n} & \cdots & a_{nm} \end{bmatrix} \begin{bmatrix} s_1(t) \\ \vdots \\ s_M(t) \end{bmatrix} \qquad (5)$$

$$s(t) = [s_1(t), s_2(t), \cdots s_M(t)]^T \quad (6)$$

$$x(t) = [x_1(t), x_2(t), \cdots x_M(t)]^T \quad (7)$$

where, **A** is the mixing matrix and **S** is an independent component. The purpose is to find **S** only using observed data **X**. Two condition should be fulfilled for smooth operation of ICA. i.e. independent component must have non-Gaussian distribution and statically independent.

3. IMAGE CRYPTOGRAPHY BASED ON MATRIX DECOMPOSITION TECHNIQUES

In this section we propose image encryption algorithm using matrix decomposition techniques given in the above section. We decomposed the input image (which is to be encrypted) using one of the matrix decompositions into a basis component matrix and its weight/strength matrix. For illustration purpose we decomposed image of size m × n into basis matrix of size m × b and strength matrix of size b × n. We can use the order reduction but that can cause the data loss and hence we use full rank decomposition in both NMF and ICA case. At the reconstruction end by operating inverse (multiplication of basis and strength matrix) operation, the reconstructed image is replica of original image.

In matrix reconstruction, its components and the order of components is very important. If the order of basis component (Columns of basis matrix) is changed, then it is impossible to reconstruct the image. We exploit this property for the image encryption purpose. In this approach, the columns of weight matrix and the row of basis matrix form the bookkeeping vector as shown in Figure 2. Also, we have added order of scrambled vectors as extra key parameter. This makes the bookkeeping vector unique, which is a major and important characteristic for encryption process. Note that, we have kept basis component, weight component and scrambling order in one stack design which is exceptional and user known only. It is ensured that, the input image can be decrypted only if the ICA, wherein the NMF is replaced by ICA matrix decomposition.

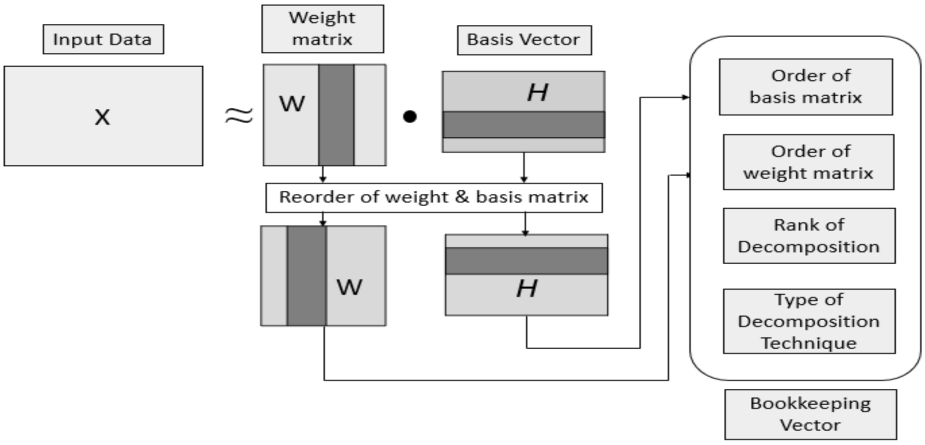

Figure 2. Key format of image encryption

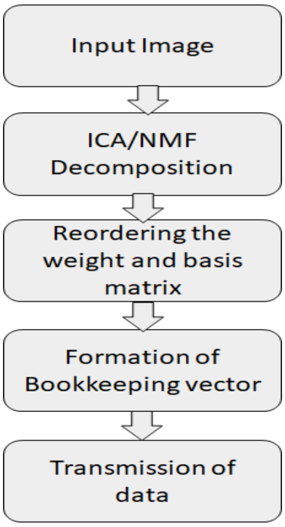
Input Image
ICA/NMF Decomposition
Reordering the weight and basis matrix
Formation of Bookkeeping vector
Transmission of data

Figure 3. Encryption workflow

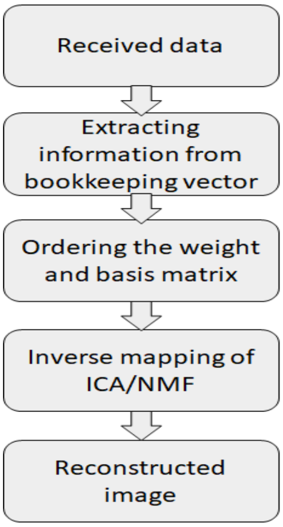
Received data
Extracting information from bookkeeping vector
Ordering the weight and basis matrix
Inverse mapping of ICA/NMF
Reconstructed image

Figure 4. Decryption workflow

The encryption procedure is explained as below:

- ➢ Read m × n input image.
- ➢ Decompose the input image using ICA/NMF method.
- ➢ Decompose the input image into basis matrix m × b and strength matrix b × n.
- ➢ Reorder the basis and weight matrix.
- ➢ Arrange the type of decomposition technique, rank of decomposition, order of basis and strength matrix in stack format of bookkeeping vector. The bookkeeping vector serve as key for encryption process.

The encryption workflow is shown in Figure 3.
Steps involve in decryption end as follows:

- ➢ Extract information (key parameters) from bookkeeping.
- ➢ Do basis and weight matrix reordering.
- ➢ Apply inverse mapping of ICA/NMF technique.

The decryption workflow is shown in Figure 4.

4. EXPERIMENTATION AND RESULTS

For experimentation purpose, we have applied the encryption algorithms given in the above section on standard images like Cameraman, Peppers, Lena, Barbara, Baboon images as shown in Figure 5(a)-(e). The size of image we have chosen is 256 × 256. The resolution of the image is 8 bits per pixel (bpp). We have done the experimentation on MATLAB and the system memory is 4 GB with Intel core 3 processor. Our encryption procedure using ICA is applied to standard images. The approximate factorization of ICA with weight/strength matrix and basis matrix is shown in Figure 5(f)-(j) and Figure 5(k)-(o) respectively and the recovered image displayed in Figure 5(p)-(t). Similarly, approximate factorization of NMF is shown in Figure 6. To enhance the complexity of key (bookkeeping vector), we scramble (reorder) the decomposed matrix columns/rows. The correlation between decomposed input image should be less [20]. Correlation coefficient determines the quality of encryption but not characterized input image. The correlation coefficients of different images are given in Table 1.

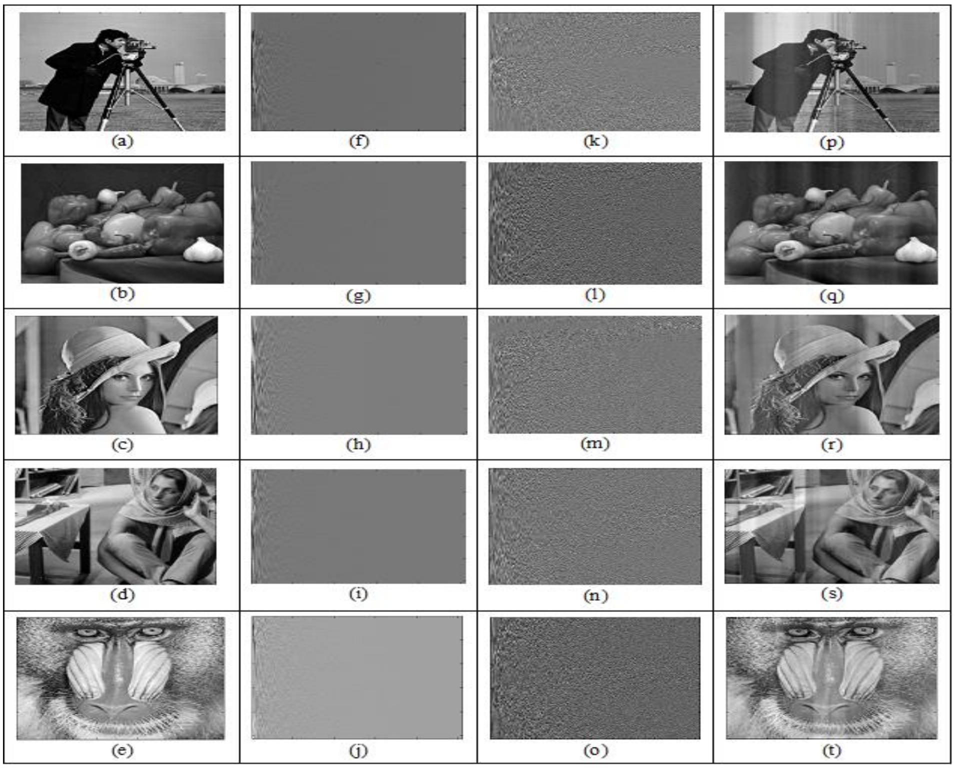

Figure 5. Simulation results. ICA: (a-e) the original images; (f-j) ICA Coefficient; (k-o) ICA Component; (p-t) ICA Reconstructed image

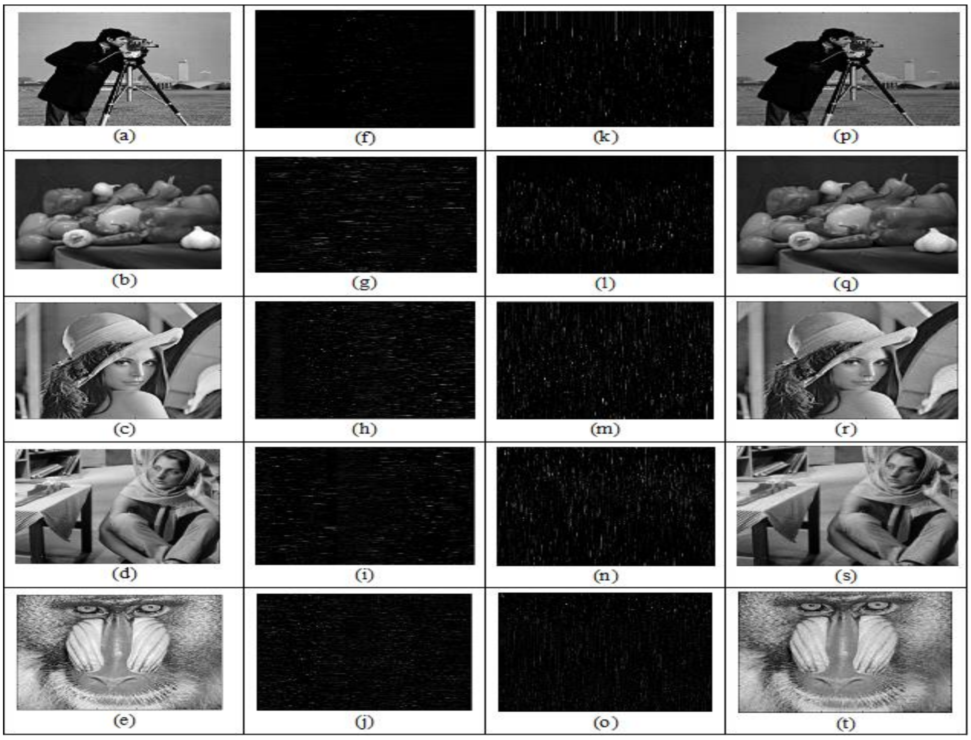

Figure 6. Simulation results. NMF: (a-e) the original images; (f-j) NMF Coefficient; (k-o) NMF Component; (p-t) NMF Reconstructed image

Table 1. Proposed correlation coefficient of image

Image	Correlation coefficient
Cameraman	0.0039
Peppers	0.0047
Lena	0.0017
Barbara	0.0038
Pout	0.0034
Baboon	0.0021

Table 2. Correlation coefficient of lena image

Image	Correlation coefficient
Proposed Method ICA	0.0017
Ref. [22]	0.0487
Ref. [23]	0.0293
Ref. [24]	0.0067
Ref. [25]	0.0019
Ref. [26]	0.0018

Table 3. Correlation coefficient of baboon image

Image	Correlation coefficient
Proposed Method ICA	0.0021
Ref. [27]	0.0075
Ref. [28]	0.0054
Ref. [29]	0.0343
Ref. [30]	0.0023
Ref. [31]	0.0026

Table 4. Encryption time analysis

Image	Encryption Time
Proposed Method ICA	0.2587
Ref. [32]	0.3827
Ref. [33]	1.2452
Ref. [34]	1.2125
Ref. [35]	0.9096
Ref. [36]	0.4071

A secured encryption technique requires high security, efficiency and high speed [21]. We have chosen Lena and Baboon image to perform the correlation analysis using ICA. we calculated the correlation between input image and basis matrix. The correlation coefficient of Lena image using ICA algorithm is tabulated in Table 2. The proposed correlation coefficient of Lena is 0.0017 which is better than state of art algorithm [22-26]. Similarly, the correlation coefficient of Baboon image using ICA algorithm is tabulated in Table 3. The proposed correlation coefficient of Baboon is 0.0021 which gives better result than the algorithm developed in the studies [27-31]. From Table 2 and Table 3, it is observed that the proposed encryption scheme has desired correlation property.

To perform the encryption time analysis, we calculated encryption time which is time between matrix decomposition to bookkeeping vector formation. We found that it takes only 0.2587 seconds to encrypt Lena image of size 256 × 256. Encrypted time analysis of Lena image with recent methods are tabulated in Table 4 shows that the proposed method is faster and encryption time is shorter than state of art encryption methods [32-36].

The performance of the proposed algorithm is better than the state of art methods. To demonstrate the effectiveness of the proposed design, we have compared the proposed techniques methods with state of art techniques in terms of correlation coefficient. It has been observed that the proposed algorithm has a relatively less correlation between the input image and the encrypted domain image.

5. CONCLUSION

This paper proposes a novel technique of image encryption based on matrix decompositions. The decompositions rank, order of decomposed component act as unique key parameters to enhance security of the system. Due to multiple user parameters, the complexity of encryption is increased and achieved data protection. It has been ensured that, the proposed encryption algorithm shows less correlation coefficient value between input and encrypted image as compared to state of art methods. Therefore, the proposed encryption algorithm has high security and strong robustness against several cryptography interferences. It is difficult to break the proposed algorithm and has low computing complications.

REFERENCES

[1] Bhandari, C., Kumar, S., Chauhan, S., Rahman, M.A., Sundaram, G., Jha, R.K., Sundar, S., Verma, A.R., Singh, Y. (2019). Biomedical image encryption based on fractional discrete cosine transform with singular value decomposition and chaotic system. 2019 International Conference on Computing, Power and Communication Technologies (GUCON), pp. 520-523.

[2] Xiong, Y., Quan, C., Tay, C.J. (2018). Multiple image encryption scheme based on pixel exchange operation and vector decomposition. Optics and Lasers in Engineering, 101: 113-121. https://doi.org/10.1016/j.optlaseng.2017.10.010

[3] Khalane, V., Bhadade, U. (2020). Image cryptography using parameterized multiband eigen wavelet filterbank. ADBU Journal of Engineering Technology, 9(1): 009010820 (7PP).

[4] Rakheja, P., Singh, P., Vig, R. (2020). An asymmetric image encryption mechanism using QR decomposition in hybrid multi-resolution wavelet domain. Optics and Lasers in Engineering, 134: 106177. https://doi.org/10.1016/j.optlaseng.2020.106177

[5] Shao, Z.H., Liu, X.L., Yao, Q.J., Qi, N., Shang, Y.Y., Zhang, J.J. (2020). Multiple image encryption based on chaotic phase mask and equal modulus decomposition in quaternion gyrator domain. Signal Processing: Image Communication, 80: 115662. https://doi.org/10.1016/j.image.2019.115662

[6] Khalane, V.P., Bhadade, U. (2017). Image encryption using wavelet transform over finite field. Proceedings of the 10th International Conference on Security of Information and Networks, pp. 257-261. https://doi.org/10.1145/3136825.3136895

[7] Lin, Q.H., Yin, F.L., Mei, T.M., Liang, H. (2008). A blind source separation-based method for multiple images encryption. Image and Vision Computing, 26(6): 788-798. https://doi.org/10.1016/j.imavis.2007.08.017

[8] Chang, H.T., Shui, J.W., Lin, K.P. (2017). Image multiplexing and encryption using the nonnegative matrix factorization method adopting digital holography. Applied Optics, 56(4): 958-966. https://doi.org/10.1364/AO.56.000958

[9] Singh, H. (2018). Watermarking image encryption using deterministic phase mask and singular value decomposition in fractional Mellin transform domain. IET Image Processing, 12(11): 1994-2001. http://dx.doi.org/10.1049/iet-ipr..5399

[10] Zafeiriou, S., Tefas, A., Buciu, I., Pitas, I. (2006). Exploiting discriminant information in nonnegative matrix factorization with application to frontal face verification. IEEE Transactions on Neural Networks, 17(3): 683-695. http://dx.doi.org/10.1109/TNN.2006.873291

[11] Lee, D.D., Seung, H.S (1999). Learning the parts of objects by non-negative matrix factorization. Nature, 401: 788-791. https://doi.org/10.1038/44565

[12] Patil, B., Panicker, M., Madhavan, R., Joel, S. (2016). Group NMF analysis for resting state fMRI. ISMRM 2016, vol, 3743.

[13] Guo, C., Jia, J., Jie, Y.M, Liu, C.Z., Choo, K.R. (2020). Enabling secure cross-modal retrieval over encrypted heterogeneous IoT databases with collective matrix factorization. IEEE Internet of Things Journal, 7(4): 3104-3113. https://doi.org/10.1109/JIOT.2020.2964412

[14] Salehani, Y.E., Arabnejad, E., Rahiche, A., Bakhta, A., Cheriet, M. (2020). MSdB-NMF: multispectral document image binarization framework via non-negative matrix factorization approach. IEEE Transactions on Image Processing, 29: 9099-9112. https://doi.org/10.1109/TIP.2020.3023613

[15] Abduldaim, A.M., Waleed, J., Mazher, A.N. (2020). An efficient scheme of digital image watermarking based on Hessenberg factorization and DWT. 2020 International Conference on Computer Science and Software Engineering (CSASE), Duhok, Iraq, pp. 180-185. https://doi.org/10.1109/CSASE48920.2020.914209

[16] Murata, N. (2016). Matrix factorization for image processing. Applied Matrix and Tensor Variate Data Analysis, pp. 73-92. https://doi.org/10.1007/978-4-431-55387-8_4

[17] Xie, S., Yang, Z., Fu, Y. (2008). Nonnegative matrix factorization applied to nonlinear speech and image cryptosystems. IEEE Transactions on Circuits and Systems I: Regular Papers, 55(8): 2356-2367. https://doi.org/10.1109/TCSI.2008.918233

[18] Dai, Y., Wang, H.Z, Wang, Y.Y. (2016). Chaotic medical image encryption algorithm based on bit-plane decomposition. International Journal of Pattern Recognition and Artificial Intelligence, 30(4): 1657001. https://doi.org/10.1142/S0218001416570019

[19] Li, S.Z., Lu, X.G., Hou, X.W., Peng, X.H. (2005). Learning multiview face subspaces and facial pose estimation using independent component analysis. IEEE Transactions on Image Processing, 14(6): 705-712. https://doi.org/10.1109/TIP.2005.847295

[20] Li, X.F., Zhang, Y.H. (2016). Digital image encryption and decryption algorithm based on wavelet transform and chaos system. 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), pp. 253-257. https://doi.org/10.1109/IMCEC.2016.7867211

[21] Khalane, V.P., Bhadade, U.S. (2018). A parameterized halfband filterbank design for image encryption. 2018 IEEE 13th International Conference on Industrial and Information Systems (ICIIS), pp. 32-35. https://doi.org/10.1109/ICIINFS.2018.8721324

[22] Hussain, S., Jamal, S.S., Shah, T., Hussain, I. (2020). A power associative loop structure for the construction of non-linear components of block cipher. IEEE Access, 8: 123492-123506. https://doi.org/10.1109/ACCESS.2020.3005087

[23] Ahmad, J., Hwang, S.O. (2015). Chaos-based diffusion for highly autocorrelated data in encryption algorithms. Nonlinear Dynamics, 82(4): 1839-1850. https://doi.org/10.1007/s11071-015-2281-0

[24] Naseer, Y., Shah, T., Attaullah, Javeed, A. (2020). Advance image encryption technique utilizing compression, dynamical system and s-boxes. Mathematics and Computers in Simulation, 178: 207-217. https://doi.org/10.1016/j.matcom.2020.06.007

[25] Naseer, Y., Shah, T., Hussain, S., Ali, A. (2019). Steps towards redesigning cryptosystems by a non-associative algebra of IP-loops. Wireless Personal Communications, 108: 1379-1392. https://doi.org/10.1007/s11277-019-06474-z

[26] Zhang, Y.Q., Hao, J.L., Wang, X.Y. (2020). An efficient image encryption scheme based on s-boxes and fractional-order differential logistic map. IEEE Access, 8: 54175-54188. https://doi.org/10.1109/ACCESS.2020.2979827

[27] Gao, W., Idrees, B., Zafar, S., Rashid, T. (2020). Construction of nonlinear component of block cipher by action of modular group PSL (2, z) on projective line PL(GF(2^8)). IEEE Access, 8: 136736-136749. https://doi.org/10.1109/ACCESS.2020.3010615

[28] Jamal, S.S., Attaullah, Shah, T., AlKhaldi, A.H., Tufail, M.N. (2019). Construction of new substitution boxes using linear fractional transformation and enhanced chaos. Chinese Journal of Physics, 60: 564-572. https://doi.org/10.1016/j.cjph.2019.05.038

[29] Idrees, B., Zafar, S., Rashid, T., Gao, W. (2020). Image encryption algorithm using s-box and dynamic hénon bit level permutation. Multimedia Tools and Applications, 79: 6135-6192. https://doi.org/10.1007/s11042-019-08282-w

[30] Attaullah, Javeed, A., Shah, T. (2019). Cryptosystem techniques based on the improved Chebyshev map: An application in image encryption. Multimedia Tools and Applications. 78: 31467-31484. https://doi.org/10.1007/s11042-019-07981-8

[31] Zahid, A.H., Al-Solami, E., Ahmad, M. (2020). A novel modular approach based substitution-box design for image encryption. IEEE Access, 8: 150326–150340. https://doi.org/10.1109/ACCESS.2020.3016401

[32] Lu, Q., Zhu, C.X., Deng, X.H. (2020). An efficient image encryption scheme based on the LSS chaotic map and single S-box. IEEE Access, 8: 25664-25678. https://doi.org/10.1109/ACCESS.2020.2970806

[33] Farah, M.A.B., Guesmi, R., Kachouri, A., Samet, M. (2020). A new design of cryptosystem based on S-box and chaotic permutation. Multimedia Tools and Applications, 79: 19129-19150. https://doi.org/10.1007/s11042-020-08718-8

[34] Zhang, X.P., Guo, R., Chen, H.W., Zhao, Z.M., Wang, J.Y. (2018). Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes. Chinese Physics B, 27(8): 080701. https://doi.org/10.1088/1674-1056/27/8/080701

[35] Çavuşoğlu, Ü., Kacar, S., Pehlivan, I., Zengin, A. (2017). Secure image encryption algorithm design using a novel

chaos based S-Box. Chaos, Solitons & Fractals, 95: 92-101. https://doi.org/10.1016/j.chaos.2016.12.018

[36] Ullah, A., Jamal, S.S., Shah, T. (2017). A novel scheme for image encryption using substitution box and chaotic system. Nonlinear Dynamics, 91: 359-370. https://doi.org/10.1007/s11071-017-3874-6