International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:9, No:1, 2015

Encryption Image via Mutual Singular Value Decomposition

Adil Al-Rammahi

***Abstract*—**Image or document encryption is needed through e-government data base. Really in this paper we introduce two matrices images, one is the public, and the second is the secret (original). The analyses of each matrix is achieved using the transformation of singular values decomposition. So each matrix is transformed or analyzed to three matrices say row orthogonal basis, column orthogonal basis, and spectral diagonal basis. Product of the two row basis is calculated. Similarly the product of the two column basis is achieved. Finally we transform or save the files of public, row product and column product. In decryption stage, the original image is deduced by mutual method of the three public files.

***Keywords*—**Image cryptography, Singular values decomposition.

I. Introduction

IMAGE or document encryption is needed through electric government and data base foundations. Really all documents are in electric form. So the designer thinks in problems of complex security. In this paper we introduce the method of mutual singular value decomposition. We have two matrices images, one is the public and denoted by a, and the second is the secret (original) and denoted by b. The analyses of each matrix is achieved using the transformation of singular values decomposition. So each matrix has row orthogonal basis and column orthogonal basis. The product of the two row basis is calculated and denoted by u. Similarly the product of the two column basis is denoted by v. Finally we transform or save the files of public a, row product u and column product v. In decryption stage, the original image is deduced by mutual method of the three public files where the inverse concept is grantee.

Many researchers work for image encryption using singular values decomposition. For updating works, EL Abbadi et al. take two images and then its spectral diagonal matrices are interchanged to new other third image [1]. Bhatnagar et al. proposed scheme to scramble the pixel positions by the means of toral automorphism and then encrypted the scrambled image using Markov map and SVD [2]. Abd El-Latif et al. proposed composed encryption method using SVD and chaotic function [3]. Tafti presents the method of Spatial Domain via SVD [4]. Wang and Chen present the method of Digital image copyright protection scheme based on SVD then on the concept of visual cryptography [5]. Rakotondraina and Razafindradina studied the famous method of Elliptic Curve Cryptosystem via SVD [6]. Devi et al. introduced Dual Image Watermarking Scheme based on Singular Value Decomposition and Visual Cryptography in Discrete Wavelet Transform [7]. Singh & S. Agarwal applied SVD on homogenous blocks via clustering technique [8]. Chanu et al. embed secret message via svd image [9].

AdilAL-Rammahi is with the Kufa University, Faculty of Mathematics and Computer Science, Department of Mathematics, Njaf, Iraq (phone: +964(0)33219195; B.O. 21 Kufa, e-mail: adilm.hasan@ uokufa.edu.iq).

II. SVD Image

Many methods of matrix analysis were studied for finding needed properties of physical problems. The theory matrix analysis based on transforming original complicated matrix to relax matrices. In singular value decomposition technique, given matrix transformed and analyzed into thee matrices where its normal product returns the original matrix. The left concerned on row basis, the right concerned on column basis, and the middle represented as diagonal form contained the squared eigen values or named as singular values. These three transformed matrices play a good role separately or in gathered. For image processing, all of these matrices were used in an algorithm for detecting the fake image without origin image [10]. The transformed middle matrix used alone in an algorithm for image compression [11].

A singular value decomposition (SVD) of real matrix $A \in R^{m\times n}, n \geq m$ is a factorization $A = U\Sigma V'$, where $U \in R^{m\times m}$ and $V \in R^{n\times n}$ are orthogonal matrices and $\Sigma = diag(s_1, s_2, ..., s_n) \in R^{m\times n}$ .The values S_i , for $i = 1,2,...,n,$ are called singular values. They may be defined to be nonnegative and nonincreasing [12]. For computational tools and reliable software, see [13].

For mathematical image, the image matrix consists of integer numbers belong to interval [0,255], see [14].

Indeed these 256 colors deduced from basic RGB colors. Each of them was transformed from its equivalent binary form and is named as a pixel. Each pixel contains 8 digits or bits(R, G, B, R+G, R+B, G+B, R+G+B, NONE). Each pixel may be appearing or not, so there are 2^8 colors which equal to 256.

For SVD matrix, all three matrices represented as fractional forms and orthogonal matrices contains negative numbers.

For SVD matrix image, we must work in carefully where the three matrices U, V, and Σ appearing in decimal form. The problem of determining the maximum and minimum of each these three matrices are difficult. Furthermore the negative numbers add another obstacle. So the method of file dealing is sensible and practical.

III. SVD Algorithm and Implementation

This section was concerned for studying the numerical method of Singular Value Decomposition (SVD) in order to

use in encryption image theory. Really we have two matrix images, one is public and denoted by a, and the second is the secret (origin) and denoted by b. The analyses of each matrix are achieved. The details of encryption and decryption stages are presented as follows.

1) Analyze $a = u_a s_a v'_a, b = u_b s_b v'_b$.
2) Calculate $u = u_a u_b, v = v_a v_b$.
3) Trans or save a , u, and v.
4) For decryption: $u_b = u_a^{-1}.u, v_b = v_a^{-1}.v$.
5) Compute b from $u_b s_a v'_b$.

For checking the powerful of proposed algorithm, many images were tested successfully. Table I was concerned for some implementations. For more deeply detecting errors, the numerical analysis and statistical measures were done to evaluate the proposed algorithm. The average correlation and the peak signal to noise ratio (PSNR) were used as the objective metrics to evaluate proposed technique. Tables II and III show the values of objective metrics between original-encrypted and original-decrypted images.

IV. Conclusion

A Numerical method of Singular Value Decomposition of matrices was used for introducing new methods for ciphering electric image. This method, and executed examples proved a good usage of analyses of Singular Value Decomposition of image encryption. First table showed that there is no different eye vision between the origin and decrypted images. In second table we notice low correlations between the origin and encrypted images. In other side there are high correlations between the origin and decrypted images where the ideal image has average correlation equal to one. Finally the errors due to the peak signal to noise ratio which appeared in the third table are encouraged to continue for working in SVD images.

TABLE I
Test Images

	Origin	Decryption		Origin	Decryption
1			6		
2			7		
3			8		
4			9		
5			10		

TABLE II
AVERAGE CORRELATION

Image	Origin & Encryption	Origin & Decryption
1	-0.0309	0.9894
2	-0.0156	0.9890
3	-0.0002	0.9728
4	-0.0098	0.9917
5	-0.0060	0.9683
6	-0.0172	0.9549
7	-0.0067	0.9727
8	0.0038	0.9771
9	0.0105	0.9647
10	-0.0251	0.9976

TABLE III
PEAK SIGNAL TO NOISE RATIO

Image	Origin & Encryption	Origin & Decryption
1	4.9121	26.1185
2	6.9481	25.5098
3	7.2953	23.8022
4	6.8444	23.3845
5	9.3448	20.4534
6	3.1916	9.1224
7	4.8416	21.6340
8	5.9526	26.2558
9	6.9093	17.3482
10	6.3389	35.7576

For more checking the accurate of our image cryptography method, the statistical detection of NPCR and UACI for origin images and its corresponding encrypted images were calculated. Those calculations were presented in Table IV. The results of all test tables are well and so the method can recommended. Image cryptography must contain two separate stages. The first is named as decryption and the second is referred as decrypted. It is the inverse of encrypted operations.

Mathematically, it is known that when small changes occur in encrypted operations tend to large changes of data information, leading to good algorithm. The famous image statistical measurements were determinate by coefficient correlation (COR), peak signal to noise ratio (PSNR), Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI). It is noted that PSNR based on the number of vanishing moments. Clearly the attacker may seek to observe variations of the encrypted image in the tiny variations of the plaintext to find the correlation between the plaintext and the encrypted image. If a tiny change in the original image can lead to a great change in the cipher image, then the algorithm can effectively resist these differential attacks. Generally, the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) can be used to describe the ability to resist the differential attack. The ideal values of NPCR and UACI are 99.61% and 33.46%, respectively. The four statistical measurements are defined as follows:

$$PSNR = 10 * \log 10 (\frac{255 * 255}{MSE}) \quad (1)$$

$$ME = \frac{1}{M * N} \sum_{i=1}^{N} \sum_{j=1}^{M} (X(i, j) - Y(i, j))^2 \quad (2)$$

$$NPCR = \frac{\sum D}{M * N} * 100 \ \% \quad (3)$$

$$UACI = \frac{1}{M * N} [\sum \frac{|X - Y|}{255}] * 100 \ \% \quad (4)$$

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

$$E(X) = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} (X(i, j) - E(X))}{M * N} \quad (6)$$

where D(i,j)=0 if X(i,j)=Y(i,j), otherwise D(i,j)=1. X and Y denote the origin image and its corresponding encryption respectively, each with dimension N*M.

TABLE IV
NPCR AND UACI OF TEST IMAGES

Image	NPCR	UACI
1	99.5361	48.8263
2	99.8660	39.8285
3	99.7063	37.4552
4	99.8502	41.4806
5	99.7912	29.9988
6	97.7971	58.8992
7	99.8097	49.0658
8	99.7599	44.7162
9	99.8422	39.4744
10	99.8183	41.9484

ACKNOWLEDGEMENT

This paper was supported by the faculty of mathematics and computer science of university of Kufa, Iraq. The author thanks all reviewers for deep reading on this paper.

REFERENCES

[1] N. EL Abbadi, A. AL-Rammahi, M. EL-Kufi "Image Encryption Based On Singular Values Decomposition", Science Publications, Journal Of Computer Science 10(7), 2014, Pp.1222-1230.

[2] G. Bhatnagar, Q. Wu, B. Raman"A Novel Image Encryption Framework Based on Markov Map and Singular Value Decomposition", Springer, Image analysis and recognition, Lecture Notes in Computer Science, Volume 6754, 2011, pp 286-296.

[3] A. Abd El-Latif ; L. Li ; N. Wang ; Q. Li ; X. Niu "A New Image Encryption Based On Chaotic Systems And Singular Values Decomposition", ProceedingsSPIE, Fourth International Conference on Digital Image Processing May 1, 2012.

[4] A. Tafti&R. Maarefdoust "Digital Images Encryption in Spatial Domain Based on Singular Value Decomposition and Cellular Automata", International Journal of Computer Science and Information Security,Vol. 11, No. 4, April, 2013, pp. 121-125.

[5] M. Wang, W. Chen, "Digital image copyright protection scheme based on visual cryptography and singular value decomposition", Optical Engineering Volume 46, Issue 6, May 2007,pp. 1-8.

[6] T. Rakotondraina& H. Razafindradina**,** **"**Authentication System Securing Index of Image using SVD and ECC", International Journal of Computer Science and Network, Vol 2, Issue 1, 2013, pp. 76-78.

[7] B. Devi, K. Singh, S. Roy**,** "Dual Image Watermarking Scheme based on Singular Value Decomposition and Visual Cryptography in Discrete

Wavelet Transform", International Journal of Computer Applications, 5(6), July 2012, PP.
[8] P. Singh & S. Agarwal, "A Visual Cryptography Based Watermarking Scheme Incorporating the Concepts of Homogeneity Analysis and Singular Value Decomposition", International Journal of Computer Applications Volume 80 , No 16, October 2013pp. 1-9.
[9] Y. Chanu, K Singh and T. Tuithung "Steganography Technique based on SVD", International Journal of Research in Engineering and TechnologyVol. 1, No. 6, 2012 .pp.293-297.
[10] N. EL Abbadi, A. AL-Rammahi, M. ELnowany "Blind Fake Image Detection", International Journal of Computer Science Issues, Vol. 10, Issue 4,No 1, July 2013, Pp.180-186.
[11] N. EL Abbadi, A. AL-Rammahi, M. EL-Kufi and D. Redha,"Image Compression Based on SVD AND MPQ-BTC", Science Publications, Journal of Computer Science 10 (10), 2104, pp.2095-2104.
[12] B. Kolman, "Introductory linear algebra with applications ", Macmillanpublishing company, New Work, 11e, 2009 .
[13] G. H. Golub and C. F. van Loan, "Matrix Computations", 3rd ed, The Johns Hopkins University Press, Baltimore, 1996.
[14] A. Bovik, "The Essential Guide To Image Processing ",Academicpress publication, 2009.

Adil AL-Rammahi was born on 1963 in Najaf, Iraq. He studied Applied Mathematics at University of Technology, Baghdad, Iraq. From the same university, he obtained his M. Sc in stability. The title of Assistant professor was awarded to him in 2002. He was awarded the degree of PhD in Fractals in 2005.He has supervised several M.Sc. dissertations. He has headed the Mathematics Department for three years from 2008-2011.His area of research is Fractals, Numerical Analysis, Cryptography and Image Processing. He published more than 25 papers and one book. He was selected as an editor, reviewer and a scientific committee member in many journals and conferences.