Journal of Computer Science 10 (7): 1222-1230, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.1222.1230 Published Online 10 (7) 2014 (http://www.thescipub.com/jcs.toc)

IMAGE ENCRYPTION BASED ON SINGULAR VALUE DECOMPOSITION

[1]Nidhal K. El Abbadi, [2]Adil Mohamad and [2]Mohammed Abdul-Hameed

[1]Department of Computer Science, University of Kufa, Najaf, Iraq
[2]Department of Mathematical, University of Kufa, Najaf, Iraq

Received 2014-01-03; Revised 2014-01-07; Accepted 2014-02-19

ABSTRACT

Image encryption is one of the most methods of information hiding. A novel secure encryption method for image encryption is presented in this study. The proposed algorithm based on using singular value decomposition SVD. In this study we start to scramble the image data according to suggested keys (two sequence scrambling process with two different keys) to finally create two different matrices. The diagonal matrix from the SVD will be interchanged with the resulted matrices. Another scrambling and diagonal matrices interchange will apply to increase the complexity. The resulted two matrices combine to one matrix according to predefined procedure. The encrypted image is a meaningfull image. The suggested method tested with many images encryption and gives promised results.

Keywords: SVD, Encryption, Image, Decryption, Image Encryption

1. INTRODUCTION

In today's world, keeping the digital information safe from being misused is one of the most important criteria. This issue gave rise to a new branch in computer science, named Information Security. Although new methods are introduced every day to keep the data secure, but computer hackers and un-authorized persons are always trying to break those cryptographic methods or protocols to fetch the sensitive beneficial information from those data. For this reason, computer scientist and cryptographers are trying very hard to come up with permanent solutions to this problem (Dey, 2012).

Security is an important issue in communication and storage of images and encryption is one of the ways to ensure security. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc.

Cryptography includes a set of algorithms and techniques to convert the data into another form so that their contents showing incomprehensible and unexplainable to anyone who not known the keys and decoded algorithm. The main aim of use of cryptographic algorithms is the protection of information and data aim of achieving privacy, Integrative the possibility of access to sources and services provided by the information system. Note that there is a set of risks which could harm the computer information systems by type of and strength of the encryption algorithm used in.

Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable.

Data encryption is a product of the information theory area of mathematics, an area that addresses various ways to manage and manipulate information. Cryptography contains two basic processes: One process is when recognizable data, called plain data, is transformed into an unrecognizable form, called cipher data. To transform data in this way is called to

Corresponding Author: Nidhal K. El Abbadi, Department of Computer Science, University of Kufa, Najaf, Iraq

encipher the data or encryption. The second process is when the cipher data is transformed back to the original plain data, this is called to decipher, or decrypting the data. To be able to determine if a user is allowed to access information a key is often used. Once a key has been used to encipher information, only someone who knows the correct key can decipher the encrypted data. The key is the foundation of most data encryptions algorithms today. A good encryption algorithm should still be secure even if the algorithm is known (Al-Husainy, 2012).

Many people consume multimedia content (images, music, movie) on portable devices like DVD player, MP3 player, Portable Multimedia Player and also through Internet. The conventional algorithms such as DES and AES cannot be used directly in multimedia data, since multimedia data are repeatedly have high redundancy, large-volumes and require real-time operations, such as displaying, cutting, copying, bit-rate conversion and so forth (Saraswathi and Venkatesulu, 2012).

It is desirable to develop an efficient image cryptosystem, especially for real-time secure image communication over open networks. To meet this challenge, a variety of image encryption schemes have been proposed.

Radha and Venkatesulu (2012), introduced a block cipher algorithm, which encrypts and decrypts a block size of 512 bits regardless of the file format. In this, a permutation algorithm using a chaotic system is employed to provide the shuffler function. A shuffler operator is defined using the shuffler function. A random key generator generates key sequences and the scheme employs key-dependant transformations based on distance in the shuffling operator. The process of encryption/decryption is governed by the shuffler function, shuffler operator and the pseudorandom key. The proposal of the algorithm is to manage the tradeoffs between the speed and security and hence appropriate for real-time image and video communication applications.

Yu (2011) have proposed image encryption technique which is based on the chaos based encryption algorithm, The algorithm uses a chaotic map base on trigonometric function as a mask to confuse the plain-image and employs several different types of operations such as right shift, left shift, XOR operation to shuffle the image pixels according to the outcome of another chaotic map. Because of this it significantly increases the resistance to statistical and differential attacks.

Enayatifar and Abdullah (2011) proposed a hybrid model which is composed of genetic algorithm and chaotic function for image encryption. In this first chaotic function logistic map is employed to separately encrypt the parts of the image. Then in the next stage these encrypted images are employed as the initial population for starting the operation of the genetic algorithm. In each stages of the genetic algorithm, the answer obtained from previous iteration is optimized so that the best encrypted image with the highest entropy and the lowest correlation coefficient among adjacent pixels is produced.

1.1. Singular Value Decomposition (SVD)

For any given matrix $A \in R^{m\times n}$ there exists a decomposition, $A = USV^T$ such that:

- U is an m×n matrix with orthonormal columns
- S is an n×n diagonal matrix with non-negative entries
- V^T is an n×n orthonormal matrix

The SVD can be performed on matrices $A \in R^{mxn}$, where $m \geq n$ (It can also be performed if $m < n$, but this is not interesting in the context of 3D Computer Vision). In the case that $m = n$ there will be only non-zero positive diagonal elements. In the case that $m > n$, $s_1,..., s_n$ are non-zero positive, sn+1,..., sm are zero. The SVD can be performed such that the diagonal values of S are descending i.e., $s_1 \geq s_2 \geq ... \geq s_n \geq 0$.

The diagonal values of S are the square roots of the eigenvalues of A^TA and AA^T (hence the non-negativity of the elements of S).

2. MATERIALS AND METHODS

2.1. Encryption

The proposed encrypt image based on SVD can be apply for both grayscale and colored images, for color image same method implemented for each color band.

Encryption method follow the following steps for each band of color image (red, green and blue):

Step1: The first step in this work is to create the necessary keys for scrambling the image data, we suggest three real keys created according to the following relations which determined by experiments:

$$[7 < key1 < 10]$$
$$[0.9 < key2 < 3 \text{ and } \text{int}(key2 * 100) \neq 150]$$
$$[0 < key3 < 3]$$

Step 2: The image values will be scrambled by using the key1 according to the following relations:

$$A1 = key1 * \max(A) - A,$$
$$A2 = key1 * \max(A1) - A1$$

Another scrambling process will be applied to the images (matrices) (A1, A2) to convert their values to extremist values; the result from this step are two matrices (B1, B2) with extremist elements, one for the positives elements while the other is for the negative elements:

$$B1 = A1 - A2,\ B2 = KEY2 * B1 + A2$$

Step3: Appling SVD for both matrices resulting from the previous step (B1 and B2).

It is clear for each matrix we get three matrices from SVD:

[UB1, SB1, VB1] = SVD (B1)
[UB2, SB2, VB2] = SVD (B2)

Step4: Rebuild new matrix from the results of SVD process in step 3, this can be done by interchange the singular values (SB) of B1 with singular values of B2:

$$C1 = UB1 * SB2 * VB1^T$$
$$C2 = UB2 * SB1 * VB2^T$$

Step5: For more complexes, the same steps above can be repeated to create new matrices. Scrambling the elements in matrices (C1, C2) to get new matrices (D1, D2):

$$D1 = C1 - C2, D2 - KEY3 * D1 + C2$$

Then, SVD applied for both matrices (D1, D2) and replaces the singular values of D1 with singular value of D2 as we did in previous steps to create new matrices (E1, E2):

[UD1, SD1, VD1] = SVD (D1)
[UD2, SD2, VD2] = SVD (D2)

So:

$$E1 = UD1 * SD2 * VD^T$$
$$E2 = UD2 * SD1 * VD2^T$$

Step6: Combine (E1 and E2) in one matrix:

$$F = [E1E2]$$

Step7: At this step we have two different choose to combine (E1 and E2):

The first choose is to reconstruct the matrix (F) by rescaling there values in the range between (0 and 1) by linear transform:

$$FF = \frac{F - M1}{MA - MI}$$

where, MA is the maximum number in matrix (F) and MI is the minimum number in the matrix (F).

These values (MA and MI) will be insert in specific locations in matrix (FF) after rescaling them to range between (0 and 1), this done by reversing four locations in the matrix (FF) for each of maximum and minimum value.

First location will be to the sign value (0.0 for positive and 0.1 for negative):

- Second location has the value = $\frac{\text{int}\left(\frac{\text{int}(\text{abs}(MI))}{255}\right)}{10000}$
- Third location has the value = $\frac{\text{remendar}(\text{int}(\text{abs}(MI)), 255)}{10000}$
- While the forth location has the value equal to the fraction of the MI number = abs (MI)-int (abs (MI)).
- The same steps applied for MA value

The second choose is to reconstruct the matrix (F) by rescaling there values in the range between (o and 255) by linear transforming:

$$FF = \frac{F - MI}{MA - MI} * 255$$

where, MA is the maximum value in the matrix (F) and MI is the minimum value in the matrix (F). Maximum and minimum values inserted in some location in matrix (FF), after scaling them to be in the range (0-255).

First location will be to the sign value (0.0 for positive and 0.1 for negative):

- The second location has the value = $\text{int}\left(\frac{\text{int}(\text{abs}(MI))}{255}\right)$
- Third location has the value = remendar (int (abs (MI))/255)
- While the forth location has the value equal to the fraction of the MI number = abs (MI)-int (abs (MI))
- The same steps applied for MA value

Encrypted image has extremist values, this feature true for all the encrypted images by this method as shown in **Fig. 1 and 2**.

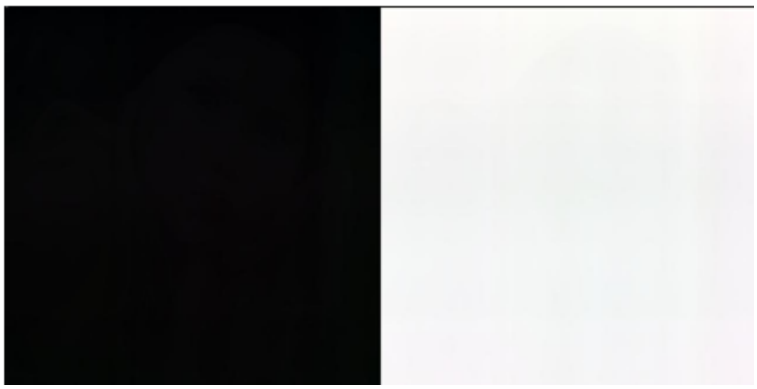

Fig. 1. Intermediate encrypted image

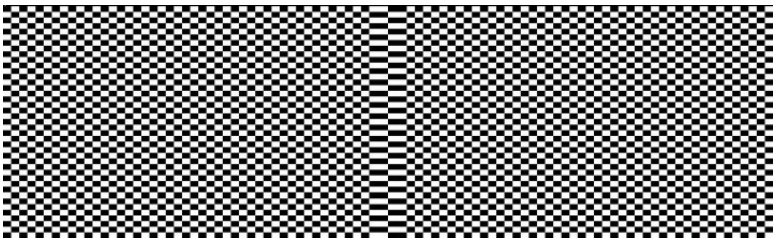

Fig. 2. Encrypted image (the final result)

Finally the encrypted image (F) will be converted to meaningful image by changing some of white region with black region according to algorithm suggested to this purpose as shown in

2.2. Decryption

The decryption process is the inverse process of encryption; at the first step we implement the algorithm to convert the encrypted image to image with two regions white and black region.

Some of the encryption keys are already store in the encrypted image such as min and max value used in rescaling the image values. It used to reconstruct the image before scaling by using the following relation:

$$FD = \frac{FF * (ma - mi)}{255} + mi$$

FD is combining of two matrices (E1 and E2), then these two matrices will be process separately.

By finding the (SVD) for both E1 and E2 we can reconstruct the matrices D1 and D2 by the same way of interchanging the diagonal matrix (S).

D1 and D2 used to reconstruct the matrices (C1 and C2) as follow:

$$C2 = D2 - Key3 * D1,\ C1 = D1 + C2$$

These matrices used to reconstruct the (B1 and B2) matrices by determine the SVD for (C1 and C2) and then interchange the S diagonal matrix for both of them.

From B1 and B2 we can determine the matrices A1 and A2 as follow:

$$A2 = B2\text{-}B1 * KEY2 \text{ and } A1 = B1 + A2$$

Finally, A can be reconstruct by using the following relation:

$$A = Key1 * \frac{\min(A1)}{Key1 - 1} - A1$$

3. RESULT

- The first example is Lena color image as shown in **Fig. 3**. PSNR for this case equal 38.2761
- The second example is the Lena gray scale image as shown in **Fig. 4**. PSNR for this case is 50.7594
- Third example is the Baboon color image as shown in **Fig. 5**. PSNR for this example is 69.877
- The forth example is for Baboon gray scale image as shown in **Fig. 6**. PSNR for this example is 51.329

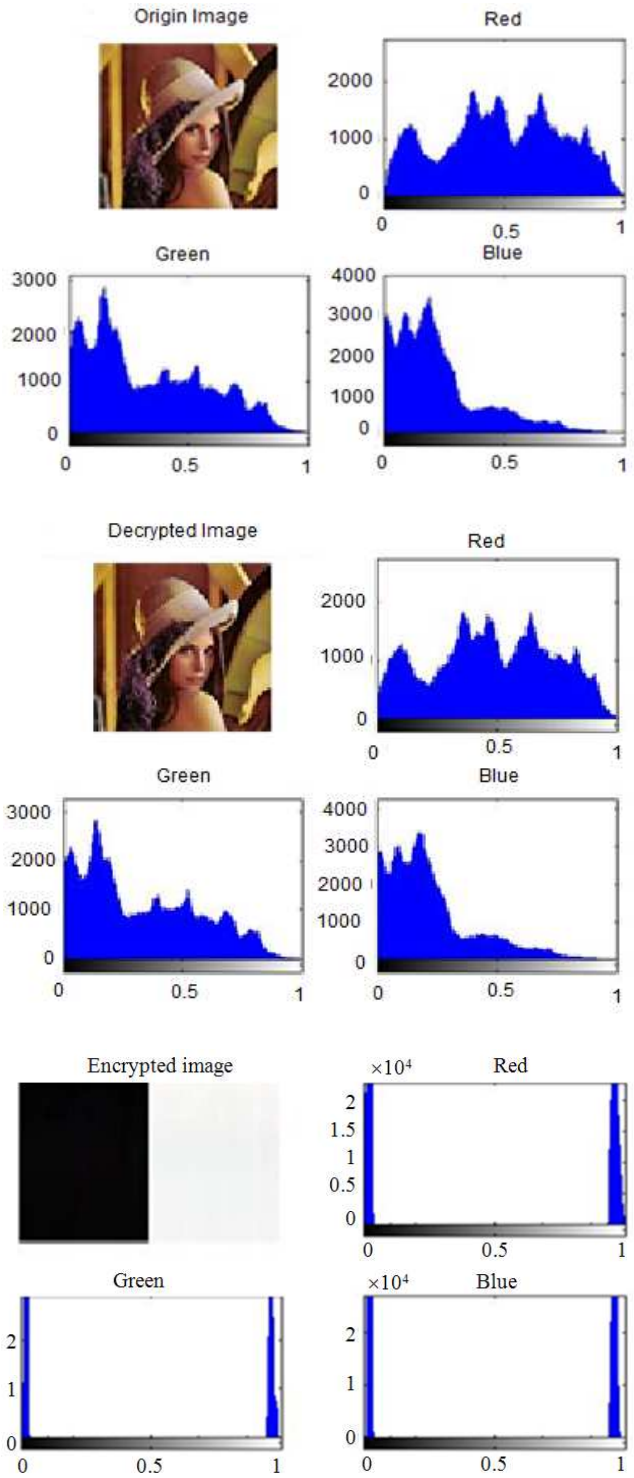

Fig. 3. Origin and decrypted lena image with corresponding histogram Encrypted image and the corresponding histogram for the three bands of encrypted image

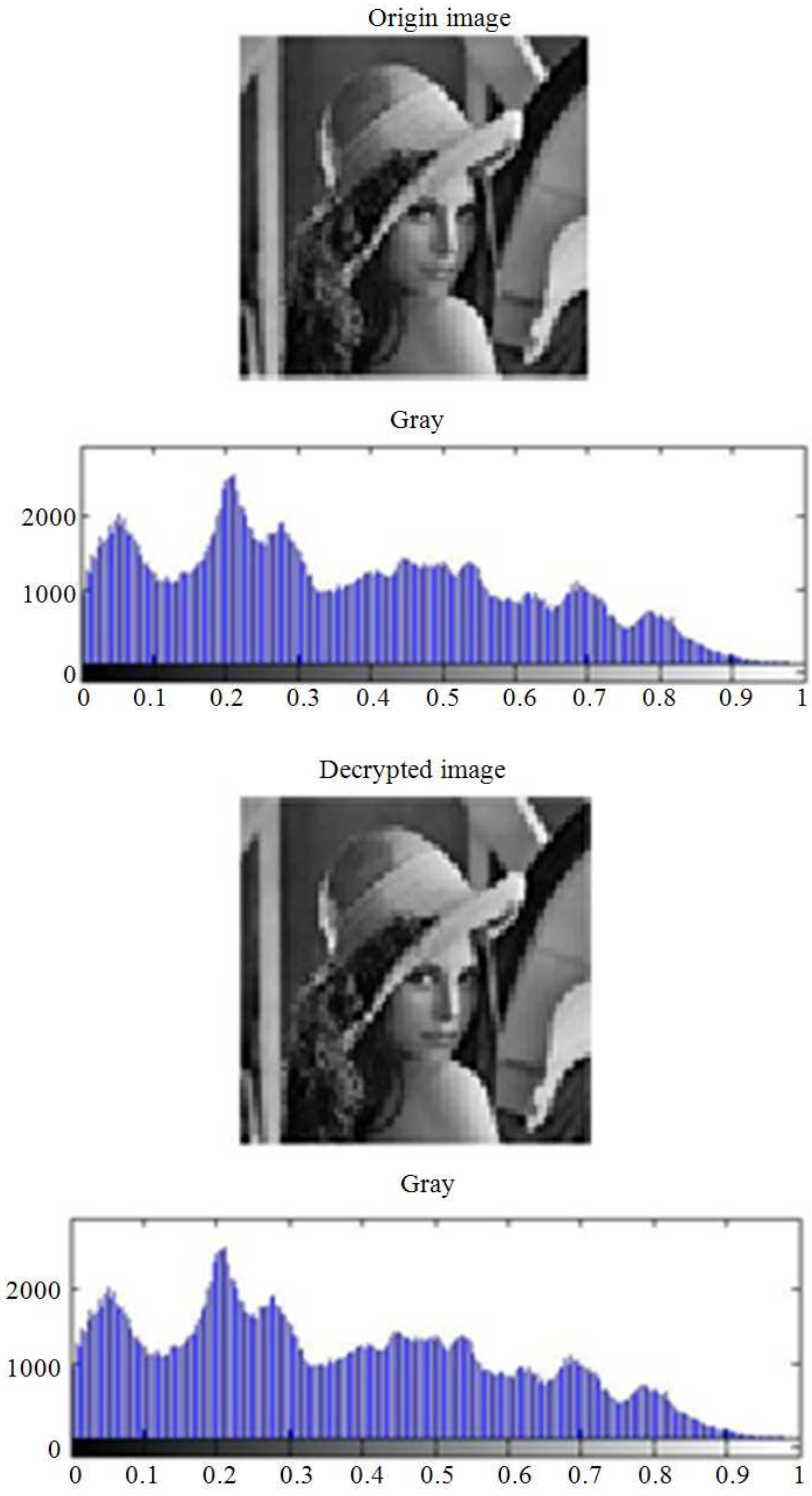

Fig. 4. Origin and decrypted Lena grayscale image with corresponding histogram

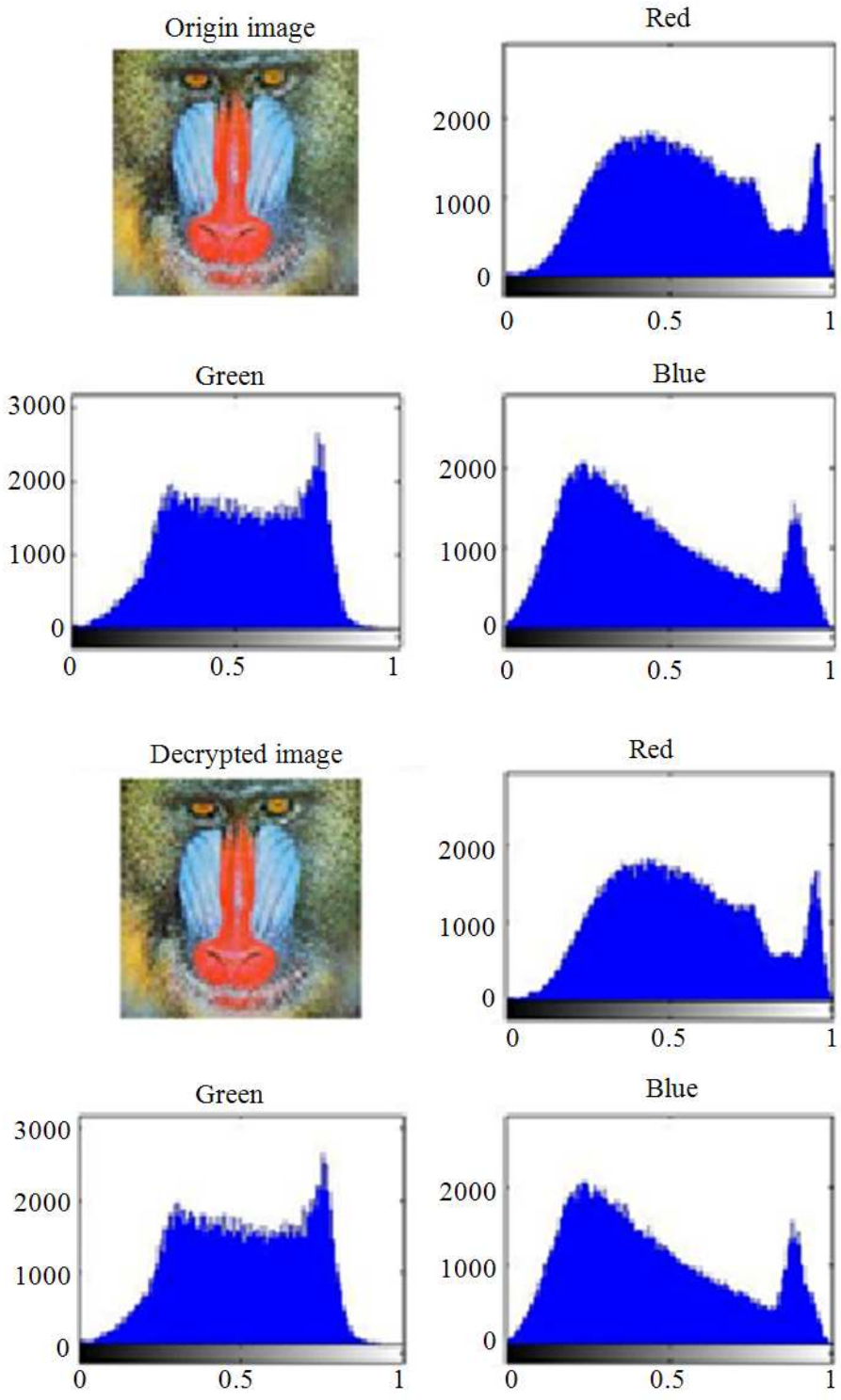

Fig. 5. Origin and decrypted Baboon color image with the corresponding histogram

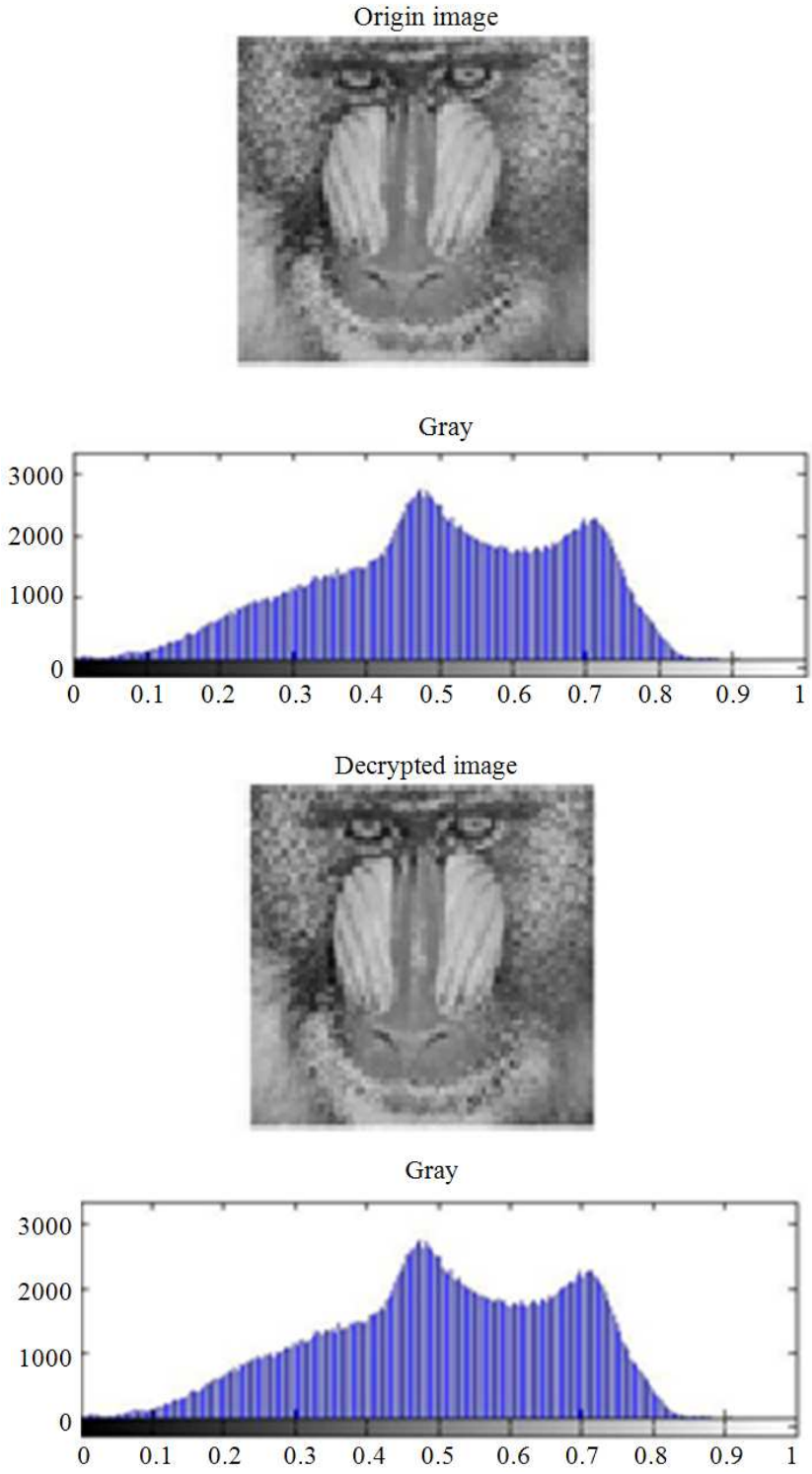

Fig. 6. Origin and decrypted Baboon grayscale image with corresponding histogram

Table 1. Comparing proposed algorithm with other algorithms

Algorithm	Image	Encryption time (s)	Decryption time (s)
MIE	Lena (grayscale)	0.270	0.22
MIE	Lena (color)	5.000	5.16
MIE	Baboon (grayscale)	0.490	0.22
MIE	Baboon (color)	9.230	9.23
VC	Lena (grayscale)	1.980	*
VC	Lena (color)	4.560	*
VC	Baboon (grayscale)	3.570	*
VC	Baboon (color)	8.350	*
Our algorithm	Lena (grayscale)	0.777	0.909
Our algorithm	Lena (color)	2.522	2.924
Our algorithm	Baboon (grayscale)	0.763	0.970
Our algorithm	Baboon (color)	2.338	3.104

* Visual cryptography exploits the human visual system to read the secret message from some overlapping shares
MIE-Mirror-like Image Encryption
VC-*Visual Cryptography*

4. DISCUSSION

The results of the proposed algorithm compared with some results of two other algorithm from paper (Ozturk and Sogukpınar, 2007) for both grayscale image and colored image, as shown in **Table 1**. The encryption and decryption time for color image work very well comparing with other algorithm, while in grayscale image the MIE is better. The proposed algorithm decrypt the image without high loss in quality as clear from the high value of PSNR.

5. CONCLUSION

In this paper, a novel simple and strong encryption method has been proposed for image security based on SVD, this is as a novel paper to encrypt image by using SVD. Image encryption techniques scrambled the pixels of the image and decrease the correlation among the pixels, so that we will get lower correlation among the pixels and get the encrypted image. In this paper we get decrypted image very close to the original image. One of the important features of this method is the encrypted images has meaningful image. Also the encrypted and decrypted time was promise when compared with other encryption techniques as in **Table 1**.

Using the SVD in encryption is new approach, we suggest as future work to use the SVD in the text encryption.

6. REFERENCES

Al-Husainy, M.A.F., 2012. A novel encryption method for image security. Int. J. Security Applic., 6: 1-8.

Dey, S., 2012. An image encryption method: SD-advanced image encryption standard: SD-AIES. Int. J. Cyber-Security Digital Forens., 1: 82-88.

Enayatifar, R. and A.H. Abdullah, 2011. Image security via genetic algorithm. Proceedings of the International Conference on Computer and Software Modeling, (CFM' 11), Press, Singapore, pp: 198-203.

Ozturk, I. and I. Sogukpınar, 2007. Analysis and comparison of image encryption algorithms. Int. J. of Inform. Technol., 1: 762-765.

Radha, N. and M. Venkatesulu, 2012. A chaotic block cipher for real-time multimedia. J. Comput. Sci., 8: 994-1000. DOI: 10.3844/jcssp.2012.994.1000.

Saraswathi, P.V. and M. Venkatesulu, 2012. A block cipher algorithm for multimedia content protection with random substitution using binary tree traversal. J. Comput. Sci., 8: 1541-1546. DOI: 10.3844/jcssp.2012.1541.1546.

Yu, C., 2011. The chaotic feature of trigonometric function and its use for image encryption. Proceedings of the 8th International Conference on Fuzzy Systems and Knowledge Discovery (KD '11), DOI: 10.1109/FSKD.2011.6019527