Available online at www.elixirpublishers.com (Elixir International Journal)

Digital Processing

Elixir Digital Processing 114 (2018) 49604-49609

ISSN: 2229-712X

An a New Algorithm Based on (General Singular Values Decomposition) and (Singular Values Decomposition) for Image Cryptography

Mohammed Abdul Hameed Jassim Al-Kufi

Department of Islamic Education, University of Kufa, 31001 Al-Najaf, Iraq.

ARTICLE INFO

Article history:

Received: 20 November 2017;

Received in revised form:

3 January 2018;

Accepted: 13 January 2018;

Keywords

Encryption,
Decryption,
SVD,
GSVD,
Image Encryption.

ABSTRACT

The issue of information security is evolving on a daily basis and the Governments in the world have become e-governments .Which makes it necessary to develop ways to maintain information to protect them from hackers and and protect them from penetration. In this paper we will encrypt the image using two well-known matrix analyzers, gsvd and svd, by relying on a complex cryptographic key, an image. The workflow will analyze the image matrix that we want to encrypt and matrix the key image using gsvd analysis.We also analyze the image matrix key using svd analysis. From the resulting matrices of the analyzes we form a new matrix through the process of constructing in a systematic manner and with new values considered large dispersion of the color values of the image matrix that we want to encrypt. This construct we have made will explain it by explaining the algorithm below. The resulting matrix represents the first and most important phase of encryption, a complex coding process that can never be broken. and to reduce the size of the last matrix to a quarter we fold it in a systematic way that can be reversed to retrieve the original values.What distinguishes this algorithm from the rest of the algorithms that preceded it is the readings that appear to the standards of global accuracy especially the encryption time, which did not exceed 1.9 seconds and the decoding time, which did not exceed 0.74 sec it is a very short period of unprecedented. We will make this clear through the tables below.

1. Introduction

Within the information security field the image is in the foreground, as the protection of the image as one of the important data you need special attention. The protection will be through encryption and in a very short time in line with the great development in this area, especially we deal with a large amount of information and data [1]. Encryption is the best way to protect data, images, texts, maps or anything, it will only be possible for the sender and the receiver to see the encrypted information because they are the only ones who know the encryption and decryption algorithm, and encryption key. Thus, cryptography can be defined as the use of mathematical algorithms to hide data in an encrypted form[2].

We can apply cryptographic algorithms to any type of data (text messages, images, or video clips) [2].

We can also define encryption as the process of converting clear data into symbols that cannot be read Except for authorized personnel. These codes are the result of the encryption process. The decryption process is the reverse of encryption in order to retrieve the original data, and this may be accompanied by an error ratio [3]. As part of the development of encryption, many technologies have been developed to encrypt texts or images and ongoing work by researchers in the development of encryption process With less time and less error [4] [5].

In the recent period science has accelerated significantly, where inventions were evolving day by day such as mobile phones. Many other functions have been developed for these inventions the increased activity of digital information exchange via Multimedia messages [6], [7], [8].

And expand the use of multimedia messages we have been forced to develop digital image technology, because they play a big role in multimedia. This requires the development of strong protections for the privacy of users, to provide them with the best services, one such means is the image encryption process to prevent hackers and unauthorized users from snooping on user privacy [9], [10] [11].

I have in my Previous research (my previous papers) (individual and joint) Seven ways to encrypt the image through seven different algorithms. Encoded image has been named as {Mk- 1 [12], Mk- 2 [12], Mk- 3 [12], Mk- 4 [12], Mk- 5 [13], MkA- 6 [14], MkHAH- 7 [5]}.

In this paper a new method of encoding has been named the encrypted image is Mk-carpet 8.

The aim of this paper is to provide high security for digital images that are sent among participants, to maintain its integrity from espionage and piracy. Also, it aims to get encryption and decryption with great precision and complexity and with the lowest time in the world.

2. SVD and GSVD.

These two analyzes of matrix is flexible matrix analyzes, which can be used in many applications, processing, compressing and encoding images. There is a detailed explanation and precise interpretations that do not concern us in this paper. For the sake of brevity and to specificity of this paper, and focus on the idea of research will suffice to refer to the idea of our paper. The reader can return to the sources we

Tele:
E-mail address: mohammeda.alkufi@uokufa.edu.iq.

refer to to learn more about them, they are very rich sources of detailed information and explanation.

2.1 SVD [12][15]

Let T be an $i \times j$ real matrix. Then there exist orthogonal matrices Q of size $i \times i$ and W of size $j \times j$ such that

$$T = QOW^T$$

Where O is an $i \times j$ matrix with nondiagonal entries all zero and:

$$o_{11} \geq o_{22} \geq \cdots \geq o_{yy} \geq 0 \; where \; y = min\{i, j\}$$

Note:

i) The diagonal entries of O are called the singular values of T.

ii)The columns of Q are called the left singular vectors of T.

iii) The columns of W are called the right singular vectors of T.

2.2 GSVD [5][16][17]

This matrix analysis larger expanded analysis svd. It is on several types, It enters into a lot of applications, within the matrices algebra field in particular, and in applied mathematics in general. In this paper, we are satisfied with clarifying it to the dear reader and making it simple, Until it is clear to him the role of this analysis in encryption.

GSVD Generalized Singular Value Decomposition. [U,V,X,C,S] = GSVD(A,B) returns unitary matrices U and V, a (usually) square matrix X, and nonnegative diagonal matrices C and S so that

$$A = U * C * X^T$$

$$B = V * S * X^T$$

$$C^T * C + S^T * S = I$$

A and B must have the same number of columns, but may have different numbers of rows. If A is m-by-p and B is n-by-p, then U is m-by-m, V is n-by-n and X is p-by-q where q = min(m+n,p).

SIGMA = GSVD(A,B) returns the vector of generalized singular values, sqrt(diag$(C^T * C)$./diag$(S^T * S)$).

The nonzero elements of S are always on its main diagonal. If m >= p the nonzero elements of C are also on its main diagonal. But if m < p, the nonzero diagonal of C is diag(C,p-m). This allows the diagonal elements to be ordered so that the generalized singular values are non-decreasing.

GSVD(A,B,0), with three input arguments and either m or n >= p, produces the "economy-sized" decomposition where the resulting U and V have at most p columns, and C and S have at most p rows.

The generalized singular values are diag(C)./diag(S). When I = eye (size (A)), the generalized singular values, gsvd(A,I), are equal to the ordinary singular values, svd(A), but they are sorted in the opposite order. Their reciprocals are gsvd(I,A).

In this formulation of the GSVD, no assumptions are made about the individual ranks of A or B. The matrix X has full rank if and only if the matrix [A; B] has full rank. In fact, svd(X) and cond(X) are equal to svd([A; B]) and cond([A; B]). Other formulations, eg.

G. Golub and C. Van Loan, "Matrix Computations", require that null(A) and null(B) do not overlap and replace X by inv(X) or inv(X^T).

Note, however, that when null(A) and null(B) do overlap, the nonzero elements of C and S are not uniquely determined.

3. Methodology of research algorithm for image encryption and decryption

3.1 Encryption

Let A_((n,m,3)) is the matrix of color values for the image we want to encrypt.

Let B_((n,m,3)) be the key image.

The dimensions of the image B should be equal to the dimensions of the image we want to encrypt A , and if not, we will modify its dimensions using a sub-program by MATLAB to dimensions A.

1- We perform the following matrix analyzes:

$$[u_1, v_1, x_1, c_1, s_1] = \text{GSVD}(A, B)$$

$$[u_2, s_2, v_2] = \text{SVD}(B)$$

2-we generate the following two matrices:

$$Z_{1(n+m,n+m,3)} = \begin{bmatrix} [(u_1)_{(n,n,3)}] & [(c_1)_{(n,m,3)}] \\ [(c_1{}^T)_{(m,n,3)}] & [(x_1)_{(m,m,3)}] \end{bmatrix}$$

and

$$Z_{2(n+m,n+m,3)} = \begin{bmatrix} [(u_2)_{(n,n,3)}] & [(s_2)_{(n,m,3)}] \\ [(s_2{}^T)_{(m,n,3)}] & [(v_2)_{(m,m,3)}] \end{bmatrix}$$

$$Z_{3(n+m,n+m,3)} = Z_{1(n+m,n+m,3)} + Z_{2(n+m,n+m,3)}$$

The dimensions of the matrix Z_3 is $(n + m, n + m, 3)$.

3-Make the matrix values of Z_3 between 0 and 255 through the linear conversion following: -

$$\text{let } t_1 = \text{minimum } (Z_3)$$

$$\text{let } t_2 = \text{maximum } (Z_3)$$

$$f_{(n+m,n+m,3)} = 255 * \frac{Z_3 - t_1}{t_2 - t_1}$$

4- Move the elements of matrix **f** to the nearest integer:

$$f_1 = int(f)$$

The rounding will be as follows:

$89.6 \approx 90$ and $89.4 \approx 89$

5-Fold rows and columns of array f_1 to halve their dimensions So that the number of its final elements is one quarter of the number before it is folded.

The following example shall be folded:

$$\begin{bmatrix} 245 & 129 & 58 & 21 \\ 98 & 177 & 254 & 200 \\ 211 & 111 & 59 & 89 \\ 233 & 10 & 244 & 44 \end{bmatrix} \rightarrow \begin{bmatrix} 245058 & 129021 \\ 98254 & 177200 \\ 211059 & 111089 \\ 233244 & 10044 \end{bmatrix} \rightarrow \begin{bmatrix} 245058211059 & 129021111089 \\ 98254233244 & 177200010044 \end{bmatrix}$$

Where we have the first step by multiplying the first column by 1000, and we have added it with the third column. And multiplying the second column at 1000, and we have added it with the fourth column and so we do with the rest of the columns in the case of large matrices.

Then the second step after the first step is to multiplying the first row in 1000000, and we have added it with the third row. And multiplying the second row in 1000000 and we added it with the fourth row and so we do with the rest of the rows in the case of large matrices.

The last matrix is $f_{2\left(\text{floor}\left(\frac{n+m}{2}\right),\text{floor}\left(\frac{n+m}{2}\right),3\right)}$

1-We create a new row in the matrix f_2 to store values t_1 and t_2 as well as n, where m represents the number of rows of the matrix of color values of the original image that we want to encrypt because we need it in the decoding process.

We will have the final matrix $f_{3\left(\text{floor}\left(\frac{n+m}{2}\right)+1,\text{floor}\left(\frac{n+m}{2}\right),3\right)}$ which represents the numerical matrix of the final encoded image.

3.2 Decryption

We have a matrix of numerical values of the encrypted image F_3.

1-From the first row we extract the value of N, T_1 and T_2 which represents the number of rows of the original image, the largest value, and the smallest value from one of the stages of encryption respectively .. Then remove the first row from F_3 to get a new matrix F_2.

2-Open the folding of matrix F_2 through reverse step (5) of the encryption be listed as follows example:

$$\begin{bmatrix}245058211059 & 129021111089\\ 98254233244 & 177200010044\end{bmatrix}\rightarrow\begin{bmatrix}245058 & 129021\\ 98254 & 177200\\ 211059 & 111089\\ 233244 & 10044\end{bmatrix}\rightarrow\begin{bmatrix}245 & 129 & 58 & 21\\ 98 & 177 & 254 & 200\\ 211 & 111 & 59 & 89\\ 233 & 10 & 244 & 44\end{bmatrix}$$

Where we made the first step by dividing the first row at 1000000, we took the Integers numbers of it and considered it the first row. After that we multiple only the fractures at 1000000 and we considered it the third row.As well as with the second and fourth grade. Thus we do with the rest of the rows in the case of large matrices.

Then we took the second step after the first step divide the first column by 1000, we took the integers numbers of it and considered it the first column. After that we multiple only the fraction at 1000. We considered it the third column. As well as with the second and fourth column, and so do with the rest of the columns in the case of large matrices.

The last matrix we call F_1.

3- We reflect the linear conversion of matrix retrieval Z_3.

$$Z_3=\frac{F_1*(T_2-T_1)+255*T_1}{255}$$

4- Conduct only one matrix analysis:

$$[U_2,S_2,V_2]=SVD(B)$$

5- We design the following matrix

$$Z_{2(n+m,n+m,3)}=\begin{bmatrix}[(U_2)_{(n,n,3)}] & [(S_2)_{(n,m,3)}]\\ [(S_2{}^T)_{(m,n,3)}] & [(V_2)_{(m,m,3)}]\end{bmatrix}$$

6- Extract the matrix $Z_{1(n+m,n+m,3)}$

$$Z_{1(n+m,n+m,3)}=Z_3-Z_{2(n+m,n+m,3)}$$

7- Of the matrix $Z_{1(n+m,n+m,3)}$ we extract matrices $U, C, \&X$ which represents the GSVD analysis of the original image matrix.

Below is a description of how to extract matrices $U, C, \&X$ in MATLAB[18].

$$U=Z_1([1:n],[1:n],:)$$
$$C=Z_1([1:n],[n+1:end],:)$$
$$X=Z_1([n+1:end],[n+1:end],:)$$

In the end, we extract the image matrix $AA_{(n,m,3)}$:

$$AA_{(n,m,3)}=U*C*X^T$$

Move the elements of matrix $AA_{(n,m,3)}$ to the nearest integer:

$$AA_{(n,m,3)}=\boldsymbol{int}(AA_{(n,m,3)})$$

The rounding will be as follows:

$89.6\approx 90$ and $89.4\approx 89$

3.3 Clarification example: -

Let $A=\begin{bmatrix}2 & 3 & 4\\ 5 & 6 & 7\end{bmatrix}\ \&\ B=\begin{bmatrix}5 & 2 & 8\\ 6 & 3 & 7\end{bmatrix}$

- **Encryption:**

$$[u_1,v_1,x_1,c_1,s_1]=GSVD(A,B)$$
$$[u_2,s_2,v_2]=SVD(B)$$

$$Z_{1(5,5)}=\begin{bmatrix}\begin{bmatrix}-0.8451 & -0.5346\\ 0.5346 & -0.8451\end{bmatrix} & \begin{bmatrix}0 & 0.5081 & 0\\ 0 & 0 & 1.0000\end{bmatrix}\\ \begin{bmatrix}0 & 0\\ 0.5081 & 0\\ 0 & 1.0000\end{bmatrix} & \begin{bmatrix}7.6304 & 1.9348 & -5.2947\\ 3.4205 & 1.3238 & -6.6744\\ 10.6124 & 0.7128 & -8.0541\end{bmatrix}\end{bmatrix}$$

and

$$Z_{2(5,5)}=\begin{bmatrix}\begin{bmatrix}-0.7052 & -0.7090\\ 0.7090 & 0.7052\end{bmatrix} & \begin{bmatrix}13.6199 & 0 & 0\\ 0 & 1.2242 & 0\end{bmatrix}\\ \begin{bmatrix}13.6199 & 0\\ 0 & 1.2242\\ 0 & 0\end{bmatrix} & \begin{bmatrix}-0.5712 & 0.5603 & -0.5998\\ -0.2597 & 0.5698 & 0.7797\\ -0.7786 & -0.6012 & 0.1799\end{bmatrix}\end{bmatrix}$$

$$Z_{3(5,5)}=Z_{1(5,5)}+Z_{2(5,5)}=\begin{bmatrix}-1.5503 & -1.2437 & 13.6199 & 0.5081 & 0\\ -0.1744 & -0.1399 & 0 & 1.2242 & 1.0000\\ 13.6199 & 0 & 7.0592 & 2.4951 & -5.8944\\ 0.5081 & 1.2242 & 3.1608 & 1.8935 & -5.8947\\ 0 & 1.0000 & 9.8338 & 0.1117 & -7.8742\end{bmatrix}$$

$$t_1=-7.8742\ ,t_2=13.6199\ ,\&\ m=2$$

$$f_{(5,5)}=255*\frac{Z_3-t_1}{t_2-t_1}=\begin{bmatrix}75.0254 & 78.6628 & 255.0000 & 99.4452 & 93.4173\\ 91.3484 & 91.7576 & 93.4173 & 107.9408 & 105.2810\\ 255.0000 & 93.4173 & 177.1655 & 123.0186 & 23.4873\\ 99.4452 & 107.9408 & 130.9162 & 115.8818 & 23.4840\\ 93.4173 & 105.2810 & 210.0827 & 94.7419 & 0\end{bmatrix}$$

$$\approx\begin{bmatrix}75 & 79 & 255 & 99 & 93\\ 91 & 92 & 93 & 108 & 105\\ 255 & 93 & 177 & 123 & 23\\ 99 & 108 & 131 & 116 & 23\\ 93 & 105 & 210 & 95 & 0\end{bmatrix}\rightarrow\begin{bmatrix}75255 & 79099 & 93000\\ 91093 & 92108 & 105000\\ 255177 & 93123 & 23000\\ 99131 & 108116 & 23000\\ 93210 & 105095 & 0\end{bmatrix}$$

$$\rightarrow\begin{bmatrix}75255255177 & 79099093123 & 93000023000\\ 91093099131 & 92108108116 & 105000023000\\ 93210000000 & 105095000000 & 0\end{bmatrix}$$

$$f_3=\begin{bmatrix}-7.8742 & 13.6199 & 2\\ 75255255177 & 79099093123 & 93000023000\\ 91093099131 & 92108108116 & 105000023000\\ 93210000000 & 105095000000 & 0\end{bmatrix}$$

- **Decryption: -**

$$f_3=\begin{bmatrix}-7.8742 & 13.6199 & 2\\ 75255255177 & 79099093123 & 93000023000\\ 91093099131 & 92108108116 & 105000023000\\ 93210000000 & 105095000000 & 0\end{bmatrix}$$

$$t_1=-7.8742\ ,t_2=13.6199\ ,\&\ n=2$$

$$f=\begin{bmatrix}75255255177 & 79099093123 & 93000023000\\ 91093099131 & 92108108116 & 105000023000\\ 93210000000 & 105095000000 & 0\end{bmatrix}\rightarrow\begin{bmatrix}75255 & 79099 & 93000\\ 91093 & 92108 & 105000\\ 255177 & 93123 & 23000\\ 99131 & 108116 & 23000\\ 93210 & 105095 & 0\end{bmatrix}$$

$$\rightarrow\begin{bmatrix}75 & 79 & 255 & 99 & 93\\ 91 & 92 & 93 & 108 & 105\\ 255 & 93 & 177 & 123 & 23\\ 99 & 108 & 131 & 116 & 23\\ 93 & 105 & 210 & 95 & 0\end{bmatrix}$$

$$Z_3=\frac{F_1*(T_2-T_1)+255*T_1}{255}=\begin{bmatrix}-1.5524 & -1.2152 & 13.6199 & 0.4706 & -0.0352\\ -0.2038 & -0.1195 & -0.0352 & 1.2292 & 0.9463\\ 13.6199 & -0.0352 & 7.0452 & 2.4935 & -5.9355\\ 0.4706 & 1.2292 & 3.1679 & 1.9035 & -5.9355\\ -0.0352 & 0.9763 & 9.8268 & 0.1334 & -7.8742\end{bmatrix}$$

$$Z_{2(5,5)}=\begin{bmatrix}\begin{bmatrix}-0.7052 & -0.7090\\ 0.7090 & 0.7052\end{bmatrix} & \begin{bmatrix}13.6199 & 0 & 0\\ 0 & 1.2242 & 0\end{bmatrix}\\ \begin{bmatrix}13.6199 & 0\\ 0 & 1.2242\\ 0 & 0\end{bmatrix} & \begin{bmatrix}-0.5712 & 0.5603 & -0.5998\\ -0.2597 & 0.5698 & 0.7797\\ -0.7786 & -0.6012 & 0.1799\end{bmatrix}\end{bmatrix}$$

$$Z_{1(5,5)}=Z_3-Z_{2(5,5)}=\begin{bmatrix}-0.8472 & -0.5062 & 0.0000 & 0.4706 & -0.0352\\ 0.5053 & -0.8246 & -0.0352 & 0.0050 & 0.9763\\ 0.0000 & -0.0352 & 7.6165 & 1.9332 & -5.3358\\ 0.4706 & 0.0050 & 3.4276 & 1.3337 & -6.7152\\ -0.0352 & 0.9763 & 10.6054 & 0.7346 & -8.0541\end{bmatrix}$$

$$U=Z_1([1:n],[1:n])=\begin{bmatrix}-0.8472 & -0.5062\\ 0.5053 & -0.8246\end{bmatrix}$$

$$C=Z_1([1:n],[n+1:end])\begin{bmatrix}0.0000 & 0.4706 & -0.0352\\ -0.0352 & 0.0050 & 0.9763\end{bmatrix}$$

$$X=Z_1([n+1:end],[n+1:end])\begin{bmatrix}7.6165 & 1.9332 & -5.3358\\ 3.4276 & 1.3337 & -6.7152\\ 10.6054 & 0.7346 & -8.0541\end{bmatrix}$$

$$AA_{(2,3)}=U*C*X^T=\begin{bmatrix}1.8380\approx 2 & 2.6446\approx 3 & 3.6346\approx 4\\ 5.0634\approx 5 & 5.9369\approx 6 & 7.1070\approx 7\end{bmatrix}\approx\begin{bmatrix}2 & 3 & 4\\ 5 & 6 & 7\end{bmatrix}=A$$

4. Application for the proposed algorithm

This algorithm can be applied to the colored and gray image with any dimensions were using MATLAB. The following is an application of this algorithm to the child's, suspended bridge, floating bridge, Lena, and Baboon images[13].

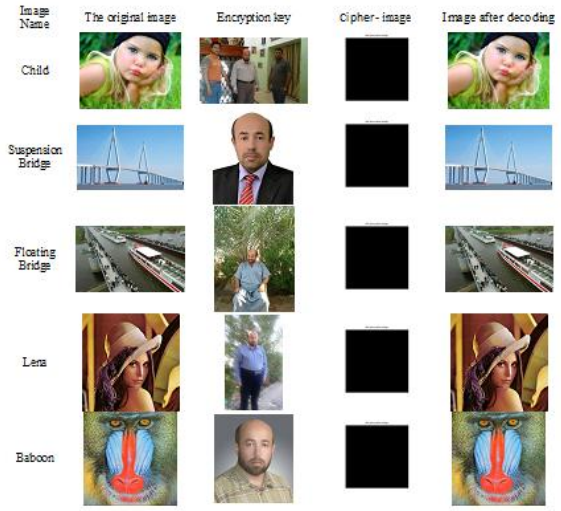

Figure 1. Sample Data Base for five images, Keys, cipher-images, and Images after decoding.

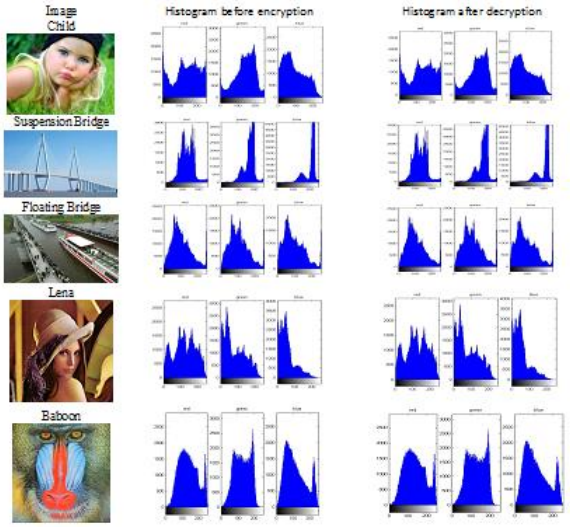

Figure 2. child's, suspended bridge, floating bridge, Lena, and Baboon images with histogram before encryption and after decryption for each red, green and blue layer matrix, with the x-axis being brightness and the y-axis being the amount of pixels.

The characterized of this algorithm that the time of encryption and decryption is very short. This is evident from the comparisons tables with other algorithms readings. In addition, the code-breaking time of a very large and undefined, where if we want to determine the time of breaking the code, we need to identify all possible possibilities for encryption and decryption key

If we can determine the total number of possibilities of decoding key we can give an approximate time to break the code. But here we use the encryption and decryption key is (color image). Thus there is a finite of possibilities for the key. Thus, the code-breaking time will be very large and undefined.

We have tried to estimate the time needed to break Lena image encryption. Which is in dimension ($512 \times 512 \times 3$). We found that we need to experience the possibilities beyond the number with (1500000) ranking, which is a very large number can not imagine and there is no computer that can be included. With paper calculations it becomes clear that we need a number of years exceeds the figure consists of (1499993) arranged for the purpose of breaking the code. This is a form of impossible.

Thus, the algorithm is a very powerful and cannot be broken..

5. Experimental Result

We extracted in this algorithm, which we called the Mk-carbit8 the encrypted image and restored the original image. We compared the original image and the image after decryption through the histogram equalization [19] [20]. As shown in Figure (2) image before encryption and after decryption, with histograms for each. It is clear the image after decryption exactly matches the original image, this is also evident from Figure (1).

So we can say that this algorithm is very good.

Table 1 Encoding and decryption time, mean error, mean squared error (MSE), peak signal-to-noise ratio (PSNR) Which have been read in this algorithm Private pictures above (floating bridge, Baboon, and Lena). These standards are defined in [10] as follows:

• Mean error is defined as the sum of all errors divided by their number.

• MSE defined as the average of errors squares, which tells you how close the gradient is to a set of points.

• Peak Signal-to-noise ratio (PSNR): indicate the peak signal to noise ratio, that a mathematical measure of the quality of the image based on the difference in pixels between the two images is equal to $10 * Log \frac{S^2}{MSE}$.

Table 1. Encryption and decryption time, mean error, (MSE), (PSNR) for (floating bridge, Baboon, and Lena) images.

Address of Reading	Name of Image		
	floating bridge	Baboon	Lena
Encryption time/s	1.25	1.898	1.799
Decryption time/s	0.53	0.74	0.73
Mean error	1.1892e-12	4.8142e-11	1.5316e-10
MSE	4.226e-24	4.4692e-21	5.0193e-20
PSNR	165.0011	149.8797	144.6276

It appears from Table 1 and through cryptographic and decoding time readings, and standards of accuracy contained in it, especially PSNR exceeding 144. There is a very large match between the original image and the image after decryption. Which confirms the quality of the proposed algorithm.

There is a global statistical accuracy standards used in image research has been used in our algorithm[21][22]. Such as:

The entropy of an image, Standard deviation, for a discrete pdf(the probability density function), Correlation coefficient, NPCR is the number of changing pixel rate, and UACI is the unified averaged changed intensity.

Table 2 shows the comparison between the statistical standards readings pre-encryption and after decryption, it shows that there is no loss of information by virtue of equal readings before and after decryption.

As shown in Table 2 readings of other statistical standards

Furthermore, table 3 shows a comparison between the readings of encryption and decryption time of our proposed algorithm with other algorithms such as MIE (Mirror-like Image Encryption) [23]; VC (Visual Cryptography) [24]; MK_1-4 (Mohammed al-Kufi—level 1-4) [12]; MK_5[13]; MKA_6[14]; MKHAH_7[5]

Table 2. Readings for the global standards accuracy before encryption and after decryption for (floating bridge, Baboon, and Lena) images.

Address of Reading	Name of Image		
	floating bridge	Baboon	Lena
Entropy before encryption	0.0074	0.003	0.1416
Entropy after decryption	0.0074	0.003	0.1416
Entropy for encryption image	0.0093	4.5305e-4	1.9015e-4
Standard deviation before encryption	55.4479	56.1909	63.8309
Standard deviation after decryption	55.4479	56.1909	63.8309
Standard deviation for encryption image	0.5212	0.4961	0.4604
Correlation coefficient between original image and image after decryption	1	1	1
Correlation coefficient between original image and encrypted image	-0.0023	-0.0034	-0.0121
NPCR	100%	100%	100%
UACI	38.4158	44.5473	29.2609

Table 3. Comparing the proposed algorithm with other algorithms.

Algorithm	Encryption time (Second)		Decryption Time (Second)	
	Image		Image	
	Lena	Baboon	Lena	Baboon
MIE	5	9.23	5.16	9.23
VC	4.56	8.35	****	****
MK-1	2.224	2.287	3.11	3.166
MK-2	5.368	5.508	6.013	6.104
MK-3	1.456	1.459	2.138	2.159
MK-4	5.54	5.567	6.265	6.382
MK-5	2.522	2.338	2.924	3.104
MKA-6	7.95	8.24	2.13	2.07
MKHAH-7	3.53	3.45	3.57	3.3
Our algorithm MK-8	1.799	1.898	0.73	0.74

(***) means that the address is not calculated

Table 4 shows a comparison between the readings of global precision standards (MSE & PSNR) for our algorithm with other algorithms.

It clearly illustrates that our proposed algorithm is excellent in terms of complexity and precision.

Table 4. Comparing the results of the global standards of accuracy (MSE) and (PSNR) with other works of image processing in general.

Algorithm	MSE		PSNR	
	Image		Image	
	Lena	Baboon	Lena	Baboon
SKM[25]JPEG	****	****	21.2	****
SKM[25]BPP	****	****	22.7	****
NKP[26]	****	****	8.67	9.076
DSA[27]	3.81e-6	****	54.18	****
TTS[28]	0.078	****	29.6041	****
AZA[29]	****	0.132977	****	56.893054
NDD[30]	0.0012	****	77.4586	****
MK-1[12]	9.9137e-26	7.9003e-26	125.0188	125.5118
MK-2[12]	9.9137e-26	7.9003e-26	125.0188	125.5118
MK-3[12]	7.3078e-27	8.9787e-27	130.6811	130.2339
MK-4[12]	9.9137e-26	7.9003e-26	125.0188	125.5118
MK-5[13]	****	****	140.4432	143.2098
MKA-6[14]	0	0	Inf	Inf
MKHAH-7[5]	7.8839e-30	****	145.5163	****
Our algorithm MK-8	5.0193e-20	4.4692e-21	144.6276	149.8797

6. Conclusions

Our algorithm (An anew algorithm based on -general singular values decomposition- and singular values decomposition for image cryptography) have the following characteristics which made them a powerful algorithm and it can be adopted in information security:

- It combines the two Algebraic matrix analyzes are (GSVD) and (SVD), which adds to the process of dispersing chromatic values further.
- Adopt both analyzes in the encryption process and then adopt one analysis which is (SVD) in the decryption process makes this algorithm same privacy as other. In addition to shortening the decoding time to approximately half the encryption time.
- Encryption key adoption is (color image) makes it hard to break the algorithm because there are an infinite number of pictures of which are considered to be a candidate encryption key. It is difficult or impossible to be broken by hackers or unauthorized.
- This algorithm can be used to encrypt any type of images including color and gray scale using MATLAB program
- This algorithm can be modified making them an ready algorithm to encrypt texts using MATLAB program as well. This is an idea for a research project to be presented later.
- From Table 1 it is clear that encryption time did not exceed 1.9 seconds. Also, the decryption time did not exceed 0.74 seconds. These are the times of record compared to the rest of algorithms. As the global standard precision (PSNR) not less than 144, it is a great read.
- Table 2 shows that this algorithm is very strong by virtue of the power of the relationship between the original image and the image after decoded, where the correlation coefficient between them is 1. It is the highest possible to arrive this parameter value. It is also evident that there is no relationship between the original image and the encrypted image because the correlation coefficient reads a negative value referring to the lack of any relationship between the two images.
- From Table 2 we see that read (NPCR) is 100%, it reference to the encryption process and changing color values is included all the color values with no part.
- Table 3 shows the time of encryption and decryption, they are standard compared to some other algorithms.
- Also table 4 indicates that this algorithm has no loss of information by virtue of reading (MSE) and (PSNR) compared to some other algorithms.

Acknowledgments:

I am very grateful, and extend my sincere thanks to Mss. 'Bushra Lateef Saddam' / director of elementary school (Almoumenat) for girls, affiliated to the Directorate of

education Kufa in Najaf to provide financial support for the completion of this research and publication. Where it expressed its willingness to provide financial support for the completion of this research free of charge for the public interest of the country.

Reference

[1] Shah, J.; Saxena, V. Performance Study on Image Encryption Schemes. IJCSI Int. J. Comput. Sci. Issues 2011, 8, 349–355.

[2] Divya, V.V.; Sudha, S.K.; Resmy, V.R. Simple and Secure Image Encryption. IJCSI Int. J. Comput. Sci. Issues 2012, 9, 286–289.

[3] Hansen, P.C. Regularization, GSVD and truncated GSVD. BIT Numer. Math. 1989, 29, 491–504.

[4] Wei, Y.; Xie, P.; Zhang, L. Tikhonov regularization and randomized GSVD. SIAM J. Matrix Anal. Appl. 2016, 37, 649–675.

[5] Mohammed Abdul Hameed Jassim Al-Kufi , Hayder Raheem Hashim , Ameer Mohammed Hussein, and Hind Rustum Mohammed; An Algorithm Based on GSVD for Image Encryption. Math. Comput. Appl. 2017, 22, 28; doi: 10.3390/mca22020028 www.mdpi.com/journal/mca

[6] M. Yang., N. Bourbakis., L. Shujun. : Data-image-video encryption. Potentials, IEEE, vol. 23, pp. 28-34, (2004)

[7] Yi, C. H. Tan., C. K. Siew., R. Syed.,: Fast encryption for multimedia. IEEE Transactions on Consumer Electronics, vol. 47, no. 1, pp. 101–107 (2001)

[8] M. Macq .,J.-J. Quisquater., : Cryptology for digital TV broadcasting. Proceedings of the IEEE, vol. 83, no. 6, pp. 944–957 (1995)

[9] S. Parker., L. O. Chua., :Chaos: a tutorial for engineers. Proceedings of the IEEE, vol. 75, no. 8, pp. 982–1008 (1995)

[10] W.Wu .,N. F. Rulkov., :Studying chaos via 1-Dmaps—a tutorial. IEEE Trans. on Circuits and Systems I: Fundamental Theory and Applications, vol. 40, no. 10, pp. 707–721 (1993)

[11]G.A.Sathishkumar ,Dr.K.Bhoopathy bagan and Dr.N.Sriraam; IMAGE ENCRYPTION BASED ON DIFFUSION AND MULTIPLE CHAOTIC MAPS; International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011

[12]Mohammed Abdul- Hameed Jassim Al- Kufi; Image Encryption with Singular Values Decomposition Aided; Msc. Thesis to Faculty of Computer Science & Mathematics- University of Kufa- 2014.

[13] Mohammed Abdul- Hameed Jassim Al- Kufi; text and image encryption via text and image keys using singular values decomposition; international journal of engineering and future technology-volume 1;issue No. 1; year 2016- ISSN 2455-6432.

[14] Adil AL-Rammahi & Mohammed Al-kufi; Image Cryptography Via SVD Modular Numbers; European Journal of Scientific Research- Volume 138 No 2 - February, 2016.

[15] Kolman B. 1984"Introductory Linear Algebra with Applications- Ninth Edition Bernard Kolman/ Drexel University-David R.Hill/ Temple University- Macmillan.

[16] Hansen, P.C. Regularization, GSVD and truncated GSVD. BIT Numer. Math. 1989, 29, 491–504.

[17] Wei, Y.; Xie, P.; Zhang, L. Tikhonov regularization and randomized GSVD. SIAM J. Matrix Anal. Appl. 2016, 37, 649–675

[18] MATLAB Version 7.12.0.635 (R2011a) 32 bit (win 32) march 18,2011 License Number 161052.

[19] Gonzalez, R.C.; Woods, R.E. Digital Image Processing, 3rd ed.; Prentice Hall: Upper Saddle River, NJ, USA, 2007.

[20] Jain, A.K. Fundamentals of Digital Image Processing Englewood Cliffs; Prentice Hall: Upper Saddle River, NJ, USA, 1989.

[21] Chaudhari, M.J.C. Design of artificial back propagation neural network for drug pattern recognition. Int. J. Comput. Sci. Eng. 2010, Special Issue, 1–6.

[22] Leung, L.W.; King, B.; Vohora, V. Comparison of image data fusion techniques using entropy and INI. In Proceedings of the 22nd Asian Conference on Remote Sensing, Singapore, 5–9 November 2001.

[23] Guo, J.I.; Yen, J.-C. A new mirror-like image Encryption algorithm and its VLSI architecture. Pattern Recognit. Image Anal. 2000, 10, 236–247.

[24] Sozan, A. New Visual Cryptography Algorithm for Colored Image. J. Comput. 2010, 2, 4

[25] Shaimaa A., Khalid F. A., Mohamed M. F. 2011. Securing Image Transmission Using In- Compression Encryption Technique. International Journal of Computer Science and Security, (IJCSS), 4(5): 466-481

[26] Narendra K P. 2012. Image encryption using chaotic logistic map, ELSEVIER. 24(9).: 926-934.

[27] Deepak A., Sandeep K., Anantdeep A. 2010. An Efficient Watermarking Algorithm To Improve Payload And Robustness Without Affecting Image Perceptual Quality, Journal of Computing.2(4). 105-109.

[28] Trinadh T., Venkata N. 2012. A Novel PSNR-B Approach for Evaluating the Quality of De-blocked Images. IOSR Journal of Computer Engineering. 4(5).: 40-49.

[29] Amira B. S., Zahraa M. T. Ahmed S. N. 2010. An Investigation for Steganography using Different Color System. Rafidain Journal of Computer Science and Mathematics for the year. Proceedings of the Third Scientific Conference on Technology of information. 29-30 / Nov. / 2010, Faculty of Computer Science and Mathematics - University of Mosul. :474-492:"
http://computerscience.uomosul.edu.iq/files/pages/page_4034788.pdf"

[30] Naitik P K., Dipesh G. K., Dharmesh N.K. Performance Evaluation of LSB Based Steganography For Optimization of PSNR and MSE. Journal of Information, Knowledge and Research in Electronics and Communication Engineering. ISSN: 0975 – 6779| NOV 12 TO OCT 13 | VOLUME – 02, ISSUE - 02 :Pages 505-509.
"http://www.ejournal.aessangli.in/ASEEJournals/EC98.pdf"